UNIVERSIDADE FEDERAL DE SANTA CATARINA
DEPARTAMENTO DE AUTOMAÇÃO E SISTEMAS

Igor Ribeiro Kuhlhoff

METHOD FOR APPLICATION OF WEIBULL DISTRIBUTION TO THE RELIABILITY CALCULATION OF FUNCTIONAL SAFETY FOR INDUSTRIAL MACHINERY

Florianópolis

2014

Igor Ribeiro Kuhlhoff

METHOD FOR APPLICATION OF WEIBULL DISTRIBUTION TO THE RELIABILITY CALCULATION OF FUNCTIONAL SAFETY FOR INDUSTRIAL MACHINERY

Dissertação submetida ao Pós-Graduação em Engenharia de Automação e Sistemas para a obtenção do Grau de Mestre em Engenharia de Automação e Sistemas.
Orientador: Prof. Dr. Ubirajara Franco Moreno

Florianópolis

2014

Ficha de identificação da obra elaborada pelo autor,
através do Programa de Geração Automática da Biblioteca Universitária da UFSC.

Kuhlhoff, Igor Ribeiro
Method for application of Weibull distribution to the reliability calculation of Functional Safety for industrial machinery / Igor Ribeiro Kuhlhoff ; orientador, Ubirajara Franco Moreno - Florianópolis, SC, 2014.
152 p.

Dissertação (mestrado) - Universidade Federal de Santa Catarina, Centro Tecnológico. Programa de Pós-Graduação em Engenharia de Automação e Sistemas.

Inclui referências

1. Engenharia de Automação e Sistemas. 2. Functional Safety. 3. Weibull. I. Moreno, Ubirajara Franco. II. Universidade Federal de Santa Catarina. Programa de Pós-Graduação em Engenharia de Automação e Sistemas. III. Título.

Igor Ribeiro Kuhlhoff

METHOD FOR APPLICATION OF WEIBULL DISTRIBUTION TO THE RELIABILITY CALCULATION OF FUNCTIONAL SAFETY FOR INDUSTRIAL MACHINERY

Esta Dissertação foi julgada aprovada para a obtenção do Título de "Mestre em Engenharia de Automação e Sistemas", e aprovada em sua forma final pela Pós-Graduação em Engenharia de Automação e Sistemas.

Florianópolis, 11 de dezembro 2014.

Prof. Dr. Rômulo Silva de Oliveira
Coordenador do Curso

Banca Examinadora:

Prof. Dr. Ubirajara Franco Moreno
Presidente

Prof. Dr. Acires Dias

Prof. Dr. Victor Juliano de Negri

Prof. Dr. Max Hering de Queiroz

AGRADECIMENTOS

Primeiramente agradeço aos meus pais, por todo o suporte incondicional desde os mais cedo momentos da vida até os dias atuais. Sem eles, nada teria sido possível. Nada. Vocês são a base do que eu sou hoje. O meu mais profundo obrigado.

Agradeço profudamente ao Alexandre Orth, meu orientador e meu amigo, idealizador do projeto, e que muito lutou para que desse certo. Obrigado por toda a ajuda, treinamentos, conversas, conselhos e caronas.

Sou grato ao Danny Koellmann, por todos os conselhos importantes sobre técnicas de apresentação e por me lembrar, sempre, de considerar o público alvo. Se a apresentação deste trabalho foi um sucesso, deve-se em grande parte ao Danny.

Sou profundamente grato ao Wouter Leusden. Ganhei um amigo dedicado, que me trouxe para o conviver com seus queridos, que me acolheu, e quem eu levarei como amizade para o resto da vida. Muito obrigado, meu amigo.

Meus agradecimentos não serão completos sem agradecer ao professor Ubirajara Moreno, pela confiança depositada, e pelas lições que mais penei e custei para aprender, já desde a época de Sinais I. Hoje reconheço o quão importante foram.

Aos meus amigos, Carolina, Ulisses, Thiago, Fernando, Gabriela, Luiz, Gelson, Juliana, Luísa, David, Olav, João, Eduardo, Thamires, James, Lucas, e mais todos que, embora não citados aqui, são igualmente importantes. Vocês tornaram esse caminho muito mais fácil. Obrigado!

À minha namorada, Milena Bettoni, por toda a compreens ao e pelo apoio. Você é única, e me deu forças para nunca desisti. Não tenho como te agradecer nem como te recompensar, por tudo o que você fez por mim, me apoiando como você me apoiou. Obrigado, de coração.

RESUMO ESTENDIDO

O desenvolvimento de sistemas elétricos e eletrônicos permitiu a massificação do uso de dispositivos eletrônicos programáveis para comando e controle de operações de sistemas técnicos. Tais dispositivos possibilitaram o desenvolvimento de sistemas técnicos mais complexos, porém, devido a essa elevada complexidade, observou-se um aumento de acidentes causados por falhas inerentes ao controle de tais sistemas. Para se reduzir esses acidentes, foram criadas normas técnicas para sistemas de controle, cuja aplicação seja relevante a segurança, o que deu origem à segurança funcional. Segurança funcional refere-se à segurança que é mantida atráves do correto funcionamento de um sistema técnico. Diferentes segmentos industriais tem aplicado o conceito de segurança funcional, para criar máquinas e sistemas mais seguros. No setor de construção de máquinas, o uso de funções de segurança reduz o número de acidentes de trabalho, ao evitar que operadores, mantenedores e pessoas ao redor fiquem expostas aos perigos inerente das máquinas. As normas técnicos impõe requisitos quantitativos e qualitativos sobre os sistemas de controle de segurança. A norma técnica internacional IEC 61508 definiu um framework para quantificação de segurança funcional. Para cada setor industrial, normas específicas foram baseadas baseadas na IEC 61508. Esse framework é bem adequado para componentes elétricos e eletrônicos. Porém, na área de maquinário industrial, sistemas de controle são realizados não somente com tais componentes, mas também por componentes mecânicos, pneumáticos e hidráulicos, os quais apresentam um comportamento diferente de falha. Tais componentes são considerados pela norma técnica internacional ISO 13849. No entanto, os métodos de quantificação desta norma contém fortes limitações e não são completamente compreendidos pelos usuários. Este trabalho dedica-se ao estudo da norma técnica internacional de segurança funcional no setor de construção de máquinas industriais, a ISO 13849. O foco do estudo é a quantificação de falhas físicas de componentes. Falhas físicas sao quantificadas através de indicadores probabilísticos, sendo objeto de estudo da engenharia de confiabilidade. No primeiro capítulo, desenvolve-se o conceito de segurança funcional. O conceito é explorado como um todo, como uma ferramenta de redução de riscos, e posteriormente como esse conceito é aplicado no setor de construção de máquinas. O apêndice A complementa o capítulo 1 com a estrutura legal no que diz respeito à segurança de máquinas na Eu-

ropa, definido pela Diretiva Europeia de Máquinas, da qual a norma técnica ISO 13849 faz parte. Ainda no capítulo 1 são identificadas as principais linhas de pesquisa, e o objetivo do trabalho é enunciado. Este trabalho, feito em parceria com a Bosch Rexroth, tem como objetivo o desenvolvimento de um método que possibilite a quatificação de índices de confiabilidade para segurança funcional utilizando distribuição de Weibull. No segundo capítulo, conceitos básicos para a compreensão do trabalho são apresentados. Os primeiros conceitos relacionam-se com conceitos da engenharia de confiabilidade, com o objetivo de esclarecer conceitos como probabilidade, confiabilidade, probabilidade de falha e construir o conceito do índice utilizado pela ISO 13849, a frequencia média de falhas perigosas por hora, PFH. O apêndice B complementa esse capítulo, com uma explicação intuitiva do que é medido através do PFH. Neste capítulo também é apresentada a distribuição de Weibull, bem como métodos de cálculo de PFH. Os parâmetros para cálculo do PFH segundo a ISO 13849 são apresentados e explicados. No terceiro capítulo é apresentado como se é calculado o PFH através de simulação a eventos discretos. Um método para cálculo do PFH considerando distribuição de Weibull, para estruturas simples e estruturas redundantes, correspondendo às categorias B, 1, 3 e 4 da norma técnica ISO 13849. O apêndices C desenvolve a equação para determinaão do número mínimo de simulações para se alcançar o resultado desejado, e o apêndice D desenvolve as equações utilizadas pelo método proposto para estruturas redundantes com falha de componentes seguindo a distribuição de Weibull. Os resultados para os casos de comparação com a ISO 13849 são apresentados no apêndice E. No quarto capítulo é apresentado um exemplo de aplicação do método proposto em uma máquina hidráulica simples do Laboratório de Sistemas Hidráulicos e Pneumáticos (LASHIP), da Universidade Federal de Santa Catarina (UFSC). A determinação do PFH e subsequentemente do PL é realizada através do procedimento dado pela norma e pelo método proposto. Utilizando-se o método proposto, foi possível calcular PFH para intervalos de utilização diferente do considerado pela ISO 13849, bem como reconhecer o efeito do desgaste do componente, caracterizado pela distribuição de Weibull. No quinto capítulo é apresentado uma visão geral de como integrar o cálculo de PFH com distribuição de Weibull com o processo de desenvolvimento de uma máquina, baseado em experiência com a Bosch Rexroth. No capítulo de conclusão é analisado o potencial de se realizar análises mais realistas, e as limitações do método proposto, sendo adequado apenas para máquinas o subsistemas produzidos em série, devido ao requerimento de dados de campo

para extrair os parâmetros da distribuição de Weibull para cada componente. Analisa-se também como que a pesquisa desenvolvida se encaixa na linha de pesquisa explicitada no primeiro capítulo, e qual a relevância para o cenário brasileiro. Adicionalmente, sugestões para trabalhos futuros são feitas.
Palavras-chave: Segurança funcional, ISO 13849, Confiabilidade, Sistema de controle de máquina

ABSTRACT

The IEC 61508 standard series defined a framework for quantification of functional safety. For each particular industry sector, specific standards are being developed based on it. This framework is well suited for electrical and electronic components. However, in the field of machinery, control systems are realized not only by such components, but also by mechanical, pneumatic and hydraulic components, which exhibit a different failure behavior. Such components are considered by the ISO 13849 standard. However, quantification methods of this standard are still not quite well understood by the users, and have strong limitations. This work presents a study an alternative method of how to calculate the average frequency of dangerous failures (PFH), required by ISO 13849 in order to achieve a Performance Level (PL). This alternative method includes modeling safety functions as Reliability Block Diagram and evaluation of PFH using the software BlockSim, through Discrete Event Simulation. Modeling hypothesis and limitations are discussed. The proposed method enables calculation of the standard's cases, as well as consideration of different failure distributions, of which Weibull distribution is considered. A study case considering Weibull distributed failures is presented. Applicability of the method is also discussed.

Keywords: Functional Safety, ISO 13849, Reliability, Machine control system

LIST OF FIGURES

Figure 1 Accident model and prevention of accident through safety barriers. Adapted from (RAUSAND, 2014) 28
Figure 2 Safety barrier classification. Adapted from Jin(JIN, 2013) 29
Figure 3 Functional blocks of a safety function 29
Figure 4 Classification of failure types 32
Figure 5 Graphical representation of table 2 35
Figure 6 Schematic representation of a hydraulic check valve. ... 42
Figure 7 Model for a a) non-repairable and b) repairable item. .. 43
Figure 8 Theoretical model of failure rate through the lifetime .. 46
Figure 9 Failure rate versus unconditional failure intensity. Adapted from Kumamoto (KUMAMOTO; HENLEY, 2000). Time axis is not in scale. 48
Figure 10 Probability Density Function of the Exponential distribution 49
Figure 11 Probability Density Function of the Weibull distribution 51
Figure 12 Failure rate of the Weibull distribution 52
Figure 13 Block diagram of a series system with two blocks 53
Figure 14 Block diagram of a parallel system with two blocks 53
Figure 15 Representation of common cause failures with Beta-factor 54
Figure 16 Graphical representation of designated architecture for category B and 1. I stands for Input element, L for Logic and O for output element. 59
Figure 17 Graphical representation of designated architecture for category 2. I stands for Input element, L for Logic, O for output element, m for monitoring, TE for test equipment and OTE for Output of the test equipment. 60
Figure 18 Graphical representation of designated architecture for category 2. I1 and I2 stands for Input, L1 and L2 for Logic, O1 and O2 for output element, m for monitoring and c for cross-monitoring. 61
Figure 19 Graphical representation of designated architecture for category 2. I1 and I2 stands for Input, L1 and L2 for Logic, O1 and O2 for output element, m for monitoring and c for cross-monitoring. Difference from figure 18 are the solid lines between L and O, de-

noting intensive monitoring. 61
Figure 20 Summary of table K.1 of ISO 13849. Reproduced from Bosch Rexroth (ORTH et al., 2012) 65
Figure 21 Differences between current method by a) ISO 13849 and b) proposed method. In b), instead of specifying $MTTF_d$ for the safety function, it is necessary to specify the parameters of Weibull distribution, η and β_W. It is also necessary to specify mission time T_M. 67
Figure 22 1oo2 RDB for category 3 or 4. Block A represents detected failures in channel 1; block B, undetected failures in channel 1; block C, detected failures in channel 2; block D, undetected failures in channel 2 and block E, failures due to common causes (CCF). 69
Figure 23 Simulation for determination of PFH. Time axis is not intended to be in scale and do not represent typical values. 69
Figure 24 Model for category B and category 1. 73
Figure 25 Representation of the determination of the failure rates for each block 78
Figure 26 Comparison of PFH values of ISO 13849 and calculated through BlockSim for all calculated categories. Intervals that represent different Performance Levels are shaded in different colors. . 81
Figure 27 Failure rate of the four analyzed cases 84
Figure 28 Failure distribution of the four analyzed cases. 84
Figure 29 PFH calculated for different mission times 85
Figure 30 Picture of the LASHIP test stand. 90
Figure 31 Schematics of the original hydraulic circuit. Reproduced from Gonzalez (GONZALEZ, 2012) 91
Figure 32 Architecture of the proposed safety function 91
Figure 33 Schematics of the proposed hydraulic circuit 92
Figure 34 Redundancy by two hydraulic valves performing a safety-related stop 92
Figure 35 5-block RBD for a redundant actuator subsystem for safety 95
Figure 36 Calculation of PFH for different components configurations and mission times. The orange area represents PL d, the red area represents PL e and the gray area has no correspondence in ISO 13849. For PFH estimation according ISO 13849, PFH is estimated just for mission time of 20 years. 98

Figure 37 Motion simulation platform built by Bosch Rexroth. . . . 102
Figure 38 Architecture of safety functions for motion platforms. Logic and output sub-functions can be realized within the scope of the deliver; input sub-function not. 111
Figure 39 Overview of activities for compliance to the Machinery Directive 112
Figure 40 Work flow for implementation of Machinery Directive for machinery and partly completed machinery. Adapted from the Guide for the Machinery Directive(GUIDE. . . , 2010) and Orth(ORTH et al., 2012). 121
Figure 41 Relation of ISO 13849 to ISO 12100. Extracted from ISO/TR 22100-2 (International Organisation for Standardization, 2013). . 125
Figure 42 Scope of ISO 12100 compared to ISO 13849 125
Figure 43 Updated work flow for compliance with Machinery Directive, considering ISO 12100 and ISO 13849 standards. 126
Figure 44 Demand of safety function in different system conditions 129
Figure 45 Demand as a failure identification process 130
Figure 46 Increase in demand rate causes the failures to be identified sooner 131
Figure 47 Use of on-line tests to reveal failures before a demand occurs 132
Figure 48 Block diagram of a series system with two blocks 139
Figure 49 Division of failures into different failure modes. Trapezoidal form are the available data, rounded rectangles are required data; dashed rectangles are only supporting understanding relations between failure modes. 141
Figure 50 Reproduction of figure 26. Comparison of PFH values of ISO 13849 and calculated through BlockSim for all calculated categories. Intervals that represent different Performance Levels are shaded in different colors. 149

LIST OF TABLES

Table 1 Comparison between nomenclature of different industry sectors functional safety standards 33
Table 2 Assignment of Performance Level according to PFH 35
Table 3 Typical reliability measures for common technologies in the machinery sector 38
Table 4 DC_{avg} classification 64
Table 5 Summary of intrinsic parameters 75
Table 6 Assignment of Performance Level according to PFH 83
Table 7 Summary of failure distribution parameters as input for case studies of a hydraulic actuator subsystem 95
Table 8 Simulation parameters 95
Table 9 Parameters for the block diagram 96
Table 10 Calculated PFH with 90% confidence interval for actuator subsystem considering mission time of 20 years 97
Table 11 Calculated PFH for the complete safety function 100
Table 12 Comparison between PFH values for category B and 1 .. 146
Table 13 Comparison between PFH values for category 3 147
Table 14 Comparison between PFH values for category 4 148

ACRONYMS AND SYMBOLS

Symbol	Description	Unity
	Latin alphabet	
CCF	Common cause failures	
DC	Diagnostic Coverage	%
DCavg	Average Diagnostic Coverage	%
E(N(t))	Expected number of failures at time t	
$\hat{E}$(N(t))	Estimate of expected number of failures at time t	
MRT	Mean repair time	hours
MTTF	Mean time to failure	Time units
MTTF$_d$	Mean time to dangerous failure	Time units
N	Number of simulations	
N(t)	Number of failures at time t	
PFD$_{avg}$	Probability of dangerous failure on demand	
PFH	Average frequency of dangerous failures per hour	$^1/_h$
PL	Performance Level	a to e
RBD	Reliability Block Diagram	
SIL	Safety Integrity Level	1 to 4
SRP/CS	Safety-related parts of Control Systems	
T_M	Mission time	Time units
	Greek alphabet	
β_{CCF}	Percentage of failures due to common causes	%
β_W	Shape factor of the Weibull distribution	
η	Characteristic lifetime of the Weibull distribution	
λ	Failure rate	
λ_d	Failure rate of dangerous failure modes	
$\lambda_d D$	Failure rate of dangerous and detected failure modes	
$\lambda_d U$	Failure rate of dangerous and undetected failure modes	
σ	Standard deviation	
$\sigma_{E(N(t))}$	Standard deviation of the expected number of failure	$^1/_h$

CONTENTS

1 INTRODUCTION 27
1.1 FUNCTIONAL SAFETY 28
1.2 FUNCTIONAL SAFETY IN THE MACHINERY SECTOR . 29
1.3 PERFORMANCE OF SAFETY FUNCTIONS 31
1.4 FUNCTIONAL SAFETY STANDARDS 32
1.4.1 Functional safety of machinery - ISO 13849 33
1.5 LIMITATIONS OF FUNCTIONAL SAFETY 35
1.6 RESEARCH AND DEVELOPMENT OF FUNCTIONAL SAFETY 36
1.7 MOTIVATION OF THE PRESENT WORK 37
1.8 OBJECTIVE 38
1.9 METHODOLOGY 39
1.10 STRUCTURE OF THE WORK 39
2 FUNCTIONAL SAFETY 41
2.1 RELIABILITY ENGINEERING 41
2.1.1 Cumulative Distribution Function 43
2.1.2 Survival Function 44
2.1.3 Probability Density Function 44
2.1.4 Failure rate 44
2.1.4.1 Failure rate curve 45
2.1.5 Mean time to failure - MTTF 45
2.1.6 B_X% life 46
2.1.7 Unconditional failure intensity 47
2.1.7.1 Difference between failure rate and unconditional failure intensity 47
2.1.8 Component reliability - Failure distributions 48
2.1.9 Lifetime distributions - Exponential 48
2.1.10 Lifetime distributions - Weibull 49
2.1.11 Availability 50
2.1.12 Unavailability 50
2.1.13 Repair rate 51
2.1.13.1 Mean Time To Repair - MTTR 51
2.1.14 System reliability 52
2.1.15 Series and parallel configuration 52
2.1.16 Common Cause Failures - CCF 54
2.1.16.1 Beta-factor model 54
2.1.17 Modeling and quantification of system reliability ... 55

2.2 SAFETY OF SYSTEMS ENGINEERING 56
2.2.1 Risk 56
2.2.2 Ratio of dangerous failure 56
2.2.3 Mission time 56
2.2.4 Average frequency of dangerous failure per hour - PFH 56
2.3 FUNCTIONAL SAFETY FOR INDUSTRIAL MACHINERY - THE ISO 13849 57
2.3.1 Categories 58
2.3.1.1 Category B 59
2.3.1.2 Category 1 60
2.3.1.3 Category 2 60
2.3.1.4 Category 3 60
2.3.1.5 Category 4 61
2.3.1.6 Custom architectures 62
2.3.2 Mean Time to Dangerous Failure - $MTTF_d$ 62
2.3.3 Average Diagnostic Coverage - DC_{avg} 64
3 ALTERNATIVE METHODS FOR PFH CALCULATION 67
3.1 HOW WAS CONSTRUCTED TABLE K.1 OF ISO 13849? 67
3.2 PFH CALCULATION BY DISCRETE EVENT SIMULATION 68
3.3 TOOLS 71
3.4 METHOD FOR CALCULATION OF PFH WITH RELIABILITY BLOCK DIAGRAMS AND SIMULATION 72
3.4.1 Model the RBD 73
3.4.2 Determine intrinsic parameters 74
3.4.3 Determine failure parameters of each block 75
3.4.4 Determine number of simulations 75
3.4.5 Convert simulation results into PFH 76
3.5 COMPARISON BETWEEN ISO 13849 AND PROPOSED METHOD 76
3.5.1 Catergory B or 1 76
3.5.2 Catergory 3 or 4 77
3.6 USE OF WEIBULL DISTRIBUTION 82
3.6.1 Catergory B or 1 with Weibull distribution 82
3.6.2 Catergory 3 or 4 with Weibull distribution 86
4 CASE STUDY OF A HYDRAULIC CONTROL SYSTEM 89
4.1 SYSTEM DESCRIPTION 89
4.2 DESIGN OF SAFETY FUNCTION 90

4.3 PFH CALCULATION ACCORDING TO ISO 13849 93
4.3.1 MTTF$_d$ 93
4.3.2 DC$_{avg}$ 93
4.3.3 Common cause failures 94
4.3.4 PFH estimation 94
4.4 PFH CALCULATION ACCORDING TO PROPOSED METHOD 94
4.4.1 Model the RBD 95
4.4.2 Determine intrinsic parameters 95
4.4.3 Determine failure parameters of each block 96
4.4.4 Determine number of simulations 96
4.4.5 Set simulation end time to mission time 96
4.4.6 Convert simulation results into PFH 97
4.5 ANALYSIS OF B_{10} 99
4.5.1 Case 200 days of operation per year 99
4.5.2 Case full year operation 99
4.6 CALCULATION OF PFH FOR THE COMPLETE SAFETY FUNCTION 100
5 APPLICATION OF PROPOSED METHOD IN AN ENGINEERING PROJECT 101
5.1 SYSTEM DESCRIPTION 102
5.2 PROJECT DESCRIPTION 103
5.2.1 Analysis of legal requirements 103
5.2.1.1 Classification under Machinery Directive 103
5.2.2 Identification of the state of the art in the technology 104
5.2.3 Identification of applicable standards 104
5.2.4 Risk assessment 104
5.2.4.1 Description of the system 104
5.2.4.2 Identification of tasks during whole life cycle 105
5.2.4.3 Identification of physical limits of machinery 105
5.2.4.4 Identification of hazards 105
5.2.4.5 Risk estimation 105
5.2.4.6 Risk evaluation 106
5.2.5 Design of safety function 106
5.2.5.1 Specify which hazards to reduce risks with each safety function 106
5.2.5.2 Define functional requirements for safety functions 107
5.2.5.3 Define required PL of each safety function 107
5.2.5.4 Design of the safety circuit 107
5.2.5.5 Obtain field failure data for components 108
5.2.5.6 Derive failure parameters from field data 108

5.2.5.7 Calculation of PFH according to methods of chapter 3 ... 108
5.2.5.8 Verification of PL ... 108
5.2.5.9 Testing of safety function for validation ... 109
5.2.5.10 Verification of achieved risk reduction ... 109
5.2.6 Preparation of documentation ... 109
5.2.7 Team definition ... 109
5.3 IMPLEMENTATION ... 110
5.3.1 Classification under the Machinery Directive ... 110
5.3.2 Risk Assessment ... 112
5.3.3 Safety functions ... 112
6 CONCLUSION ... 115
6.1 IMPORTANCE ... 115
6.2 SUGGESTION FOR FUTURE WORKS ... 117
APPENDIX A – Framework for safety of machinery ... 121
APPENDIX B – Intuitive interpretation of PFD_{avg} and PFH ... 129
APPENDIX C – Deduction of equation for the number of simulations ... 135
APPENDIX D – Deduction of equations for failure parameters of the 5-block model ... 139
APPENDIX E – Analysis of error for validation ... 145
References ... 151

1 INTRODUCTION

With the growing complexity of automated systems, there has been an increase in the number of severe accidents causing great commotion. A crash-landing in San Francisco in 2013 (TRAUFETTER, 2013), overexposure to Cobalt-60 in San Jose in 1996(IAEA, 1998), a crash-landing without steering capabilities in Iowa in 1989 (NTSB, 1990) and the radiation overdoses caused by the machine Therac-25 in 1985 (LEVESON, 1995) are some examples of disasters triggered by failures in the control system. Physical failures of components, software bugs and interaction of environmental and operation conditions cause the system to behave in an unexpected and undesired way.

Technical systems do not cause only big accidents. Machines are also responsible for a great number of work accidents, that while not so disastrous, they are certainly much more frequent and have huge losses as well. According to the Annual Report of the Brazilian Social Security (MINISTéRIO DA PREVIDêNCIA SOCIAL, 2014), ca. 717.9 thousand work accidents, of which approximately 555.1 thousand were typical work accidents[1]. From the total amount of work accidents, industry is responsible for 45.48% of accidents.

Our society benefits of such dangerous system. In order to enable safely operation of such dangerous systems, it is therefore mandatory to reduce risks of accidents. Systems have to be designed not only to fulfill their intended function, but also to avoid unsafe conditions, processes failures and instabilities. Different design measures can be used for that, what are called *safety barriers*. Safety barriers are physical and non-physical means of preventing, controlling and mitigating accidents (SKLET, 2006).

A single safety barrier would ideally prevent all accidents. However, safety barriers can be designed to prevent only foreseeable accidents, may have design flaws and other failures that impair its correct operation. From this reason, different safety barriers are combined to reduce even more the chance of an accident.

Figure 1, adapted from Rausand (RAUSAND, 2014), represents a model for an accident. A source of hazard is contained by safety barriers. “Holes” in barriers represent unforeseen conditions or failures. A

[1]Due to Brazilian law 8213/91, occupational diseases and traffic accidents between workplace and residence are also considered work accidents and are counted in the statistics by the National Institute for Social Security, the *Instituto Nacional do Seguro Social, INSS*.

hazardous situation, caused by the hazard source, is an potential accident, that is to be contained by a safety barrier. A hazardous situation is seen as a demand for the safety barrier. Through "holes" in each barrier, demands are reduced to next barriers, until the last barrier, where remaining hazardous situations can lead to an accident. It is of interest of safety engineering to quantify how big are such "holes".

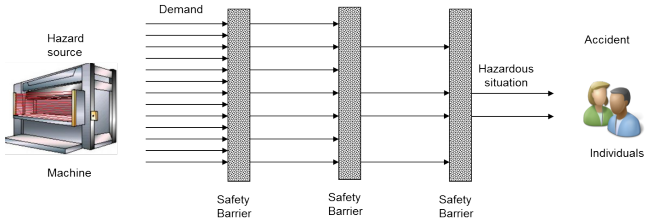

Figure 1 – Accident model and prevention of accident through safety barriers. Adapted from (RAUSAND, 2014)

1.1 FUNCTIONAL SAFETY

Not every safety barrier is implemented in the same way, or has the same effect on the technical system. A safety barrier can be isolation through fences or housing of a hazard source, can be a procedure in case of emergency or can be an automatic system.

A classification of safety barriers is given by Sklet (SKLET, 2006), and represented in figure 2. A first classification is whether a safety barrier is active or passive. To passive safety barrier belong, among others, fences and safety inherent design concepts. To active barriers belong, among others, automatic systems for accident avoidance and calling firefighters, for example.

Following figure 2, an automatic system for accident avoidance is implemented by a technical system, opposing to an administrative barrier, as calling firefighters or having special procedures for emergency situations. For technical systems, that implement a safety barrier in an active manner, it is said that this system implements a *safety function*. A safety function is therefore a sub-group of safety barriers.

Functional safety is the denomination to the knowledge area that deals with safety functions.

From the perspective of an automatic system, function means an action or set of actions that this system performs in order to achieve

a desired effect to an external environment, as exposed by De Negri (NEGRI, 2005). A first attempt then to understand functional safety is to think of a function of a dedicated control system to reduce risks inherent of a process or a system. These terms are better described through the next chapter.

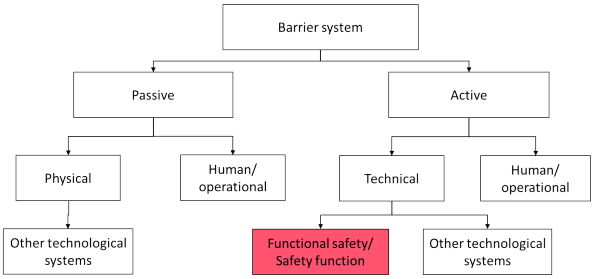

Figure 2 – Safety barrier classification. Adapted from Jin(JIN, 2013)

Functional safety is characterized by the active operation of a system, in order to maintain the safe condition. A general structure of a safety function is represented in figure 3. The safety function has to detect the dangerous condition or event, decide what is the suitable reaction, and act in the system or process, what is called a *safety loop*.

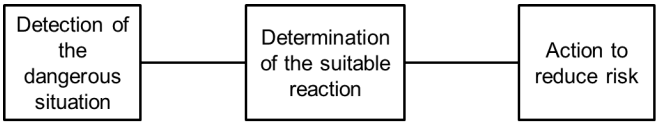

Figure 3 – Functional blocks of a safety function

An example of functional safety is an emergency shutdown system of a chemical plant. A special system monitors pressure of a pipeline, and in the case of over-pressure (over safe limits), due some problem or instability, this special system takes over and shut down the plant, or a part of it, to avoid accidents to happen (RAUSAND, 2014).

1.2 FUNCTIONAL SAFETY IN THE MACHINERY SECTOR

Workplace accidents involving machinery normally do not have large proportions like the above mentioned, although they are much more frequent. Together with high costs, there is intention to increase

workplace conditions and to reduce accidents. In the field of machinery, the European Machinery Directive 2006/42/EC (EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION, 2006) has assigned machine builders the responsibility of providing a safe machine. They became liable for accidents caused by an unsafe machine. In Brazil, the revision of the Norma Regulamentadora 12 - NR12 (MINISTERIO DO TRABALHO E EMPREGO, 2013) in 2010 pursues the same objective.

The Machinery Directive defined a legal framework for safety, as well as Essential Health and Safety Requirements. Its fulfillment has to be adopted in the European countries as law. Technical standards, whose application is not mandatory, provide solutions to design of safe machines. There are different measures that can be adopted. Functional safety is one of them. For a deeper discussion on the Machinery Directive, refer to appendix A.

Safety functions in the machinery sector mostly prevent access to moving parts, or to avoid accidents before they occur. While in the case of process industry, where a safety system monitors operational parameters and acts in the case of a deviation, in the machinery sector safety functions control directly the hazards (e.g moving parts) and can steer them to a safe state when the presence of a person is detected.

The scope of functional safety in the machinery sector is to reduce risks of hazards arising from unexpected, unpredictable and uncontrollable movements.

As an example, consider a machining center, as described by "10 Steps to Performance Level" (ORTH et al., 2012). The working area, where the cutting tools move, is protected by a door. The door protects persons entering the hazardous area, i.e. where the cutting tools can move. If some opens the door, the cutting tools have to stop, in order to prevent an accident. The safety function, in this case, is **stop machine tool movements**, triggered by opening of the door.

A second example, considering the same machine, is setup of work-pieces. In this case, it is assumed that is necessary to keep the door open, while moving the cutting tool. In order to reduce risks of accidents, the cutting tool shall move at reduced speed. The safety function, in this case, is **moving with reduce speed**, triggered by a special operation mode. The safety-related system must **monitor** the tool speed, for the case a failure causes the tool to move faster than allowed. If this happens, machine tool movements must stop, in order to maintain the overall safety.

1.3 PERFORMANCE OF SAFETY FUNCTIONS

The indiscriminate use of a safety function does not alone guarantee the avoidance of the accident. In order to be effective, it has to be carefully designed. Sklet (SKLET, 2006) defines different ways of evaluating a safety barrier or a safety function. Among them, the performance measure of interest for this work are:

- Effectiveness
- Integrity

Effectiveness is related to the behavior of the safety-related part of the system, whether the reaction is suitable or not, and if all conditions or events were considered. In other words, it is equivalent to the question: "Does the (safety) system do the right thing?" A safety function has to be described in a document, in terms of what are its requisites, when it shall act (whether continuous or to react an event), its response times, the reaction, the safe state that it should bring the system, etc.

Integrity is related to its robustness against failures (of the safety function), and in the case of a failure, how the safe state is maintained. In other words, it is equivalent to the question: "Can the safety system do the right thing?" Integrity is quantified in terms of probabilistic indicators and complementary requirements.

Integrity is impaired by, among other causes, failures of safety components and faults and errors of safety software. These causes have different nature and affect the safety function in different ways. Therefore, a classification between fail-to-function causes is proposed in figure 4. A first differentiation is made whether the safety function failed to function due to a component failure or a software ERROR. This differentiation between the sources of incapability of the safety function reflects whether the system has lost the capability of controlling/acting due to lack of "hardware" or if it has the "hardware" but does not react in a proper way.

A further differentiation of the fail-to-function cause is possible, as shown in figure 4. For component failures, a distinction between early, random and wear out failures is made. This differentiation is explored in the next sections. A differentiation between software errors and systematic failures is illustrative and as they do not influence in the quantification, they are not further explored in this work.

This differentiation reflects in the safety assessment to each cause. Component failures are quantifiable by probabilistic indicators.

Software errors and systematic failures are qualitatively assessed.

For the quantifiable failures, two commonly used probabilistic indicators are:

- *Average probability of failure on demand - PFD_{avg}*
- *Average frequency of dangerous failures - PFH*

These measures are better explained in Chapter 2 and in appendix B. Together with complementary requirements, these measures define integrity levels, which are determined by standards.

1.4 FUNCTIONAL SAFETY STANDARDS

Due to its criticality, an important characteristic of functional safety is its regulation by standards. Standards provide design principles, qualitative requirements, procedures for determination of PFD_{avg} and PFH, checklists, guide the documentation and define target values for integrity measures, which enables comparison between different systems and solutions (GOBLE, 2010).

Menis and Buja (BUJA; MENIS, 2012) say that "functional safety standards focus on the characteristics of the means added to a system to ensure its safety, where the means are constituted by hardware and/or software devices. The added means are commonly termed extra systems since they are not necessary to deliver the intended service, apart from the safety."

There are a number of different standards, each one intended to a different sector. The first standard was the IEC 61508, whose first version was issued in 1998, and was revised in 2010. This standard sets a general framework for functional safety, which was adapted to different sectors, given birth to sector-specific standards. The IEC 61508 has

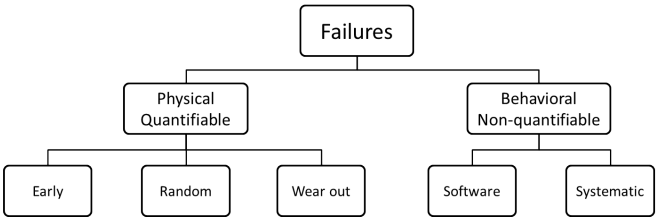

Figure 4 – Classification of failure types

7 parts, and defines a safety life cycle concept, where integrity of safety functions is planned, designed and maintained through the process or system life (Quality Management System for Safety) (RAUSAND, 2014).

As each standard adopts its own terms, confusion may arise, specially when the scope of application lies between two standards. While a safety system is called Electrical/ Electronic/ Programmable Electronic (E/E/PE) Safety-related Systems in the IEC 61508, in the process industry it is called Safety Instrumented System (SIS), in the machinery industry by Safety Related Electrical Control System (SRECS) by IEC 62061 and Safety Related Parts of Control System (SRP/CS) by 13849. Automotive industry refers to the safety system as Electrical and Electronic Safety-related system, while in nuclear industry it is called by Instrumentation and Control System. For the target measures, Safety Integrity Level (SIL), Performance Level (PL) and Automotive Safety Integrity Level (ASIL) are used.

A brief comparison between the functional safety standards is given in the table 1[2], as a tentative of clarification.

Table 1 – Comparison between nomenclature of different industry sectors functional safety standards

Standard	Sector	Denomination of the control system	Target measure
IEC 61508	General framework	E/E/PE Safety-related system	SIL
IEC 61511	Process industry	SIS	SIL
IEC 62061	Machinery	SRECS	SIL
ISO 13849	Machinery	SRP/CS	PL
ISO 26262	Automotive	E/E Safety-related system	ASIL
IEC 61513	Nuclear Power	I&C system	-

The focus of this work is the standard ISO 13849. Therefore, its terms are adopted from now on.

1.4.1 Functional safety of machinery - ISO 13849

In the field of machinery, safety standards started to be developed before the IEC 61508. The first machine safety standard was the EN 954 in 1996, which had a qualitative approach to ensure the in-

[2]The standards listed in the table are issued by international committees as ISO and IEC, and are widely accepted in Europe. Some other country are adopting these standards as well, as Brazil, through the ABNT. In the USA, the IEC 61511 is adopted as ANSI/ISA 84.00.01 about Safety Instrumented Systems for process industry

tegrity of the controls of machinery, based in the years of experience in design. The concept of category was created, which described the behavior of the control system in presence of a fault (LERéVéREND, 2008).

A large number of machine specific standard were developed under this concept of categories, what has made it a successful standard. Machine builders had standard solutions for the safety of control systems. However, there was no mention to programmable systems, which should be designed following the recommendations of the predecessor of IEC 61508.

Publication of IEC 61508 had a huge impact in many industry sectors. It defined what is known today as functional safety. It triggered efforts to bring these concepts and techniques to the machinery sector. The IEC 62061 is the application of the IEC 61508 framework to the machinery sector, with a more detailed approach requiring mastery of reliability evaluation techniques. However, this approach is limited to electrical, electronic and programmable components.

Approximately at the same time, an European project called *Standards for Safety Related Complex Electronic Systems - STSARCES* (DORRA; REINERT, 2000) made an investigation in complex electronic and programmable systems for the machinery sector. It was an attempt to achieve a SIL for the categories of EN 954.

In 2006, ISO 13849 was published, based on findings of the STSARCES project. It maintained much of the structure of the EN 954 while introduced reliability concepts and calculation. Due to the number of machine standards that were already based on the EN 954, ISO 13849 conserved the structure of categories, while introduced simplified and customized reliability estimation methods. The standard remained therefore compatible with the old machinery standards, and provided an easier way to estimate the integrity of a safety function in the design phase. These factor made it very popular and widely accepted.

The ISO 13849 is a standard on functional safety for the machinery sector. It defines five *Performance Levels - PL*, named from *a* to *e*, being e the level with highest integrity. The PL is defined in terms of qualitative and quantitative requirements. Referring to figure 4, it can be roughly said that quantitative requirements relate to reduction of component failures, while qualitative for reduction of software errors and systematic failures. For the quantitative, the PFH has to be calculated. The table 2 shows the correspondence of PFH to PL. For a graphical representation of range of PFH values and correspondence to

PL, see figure 5.

Table 2 – Assignment of Performance Level according to PFH

Performance level (PL)	Average Frequency of Dangerous Failure per Hour (PFH)
a	$\geq 10^{-5}$ to $< 10^{-4}$
b	$\geq 3 \cdot 10^{-6}$ to $< 10^{-5}$
c	$\geq 10^{-6}$ to $< 3 \cdot 10^{-6}$
d	$\geq 10^{-7}$ to $< 10^{-6}$
e	$\geq 10^{-8}$ to $< 10^{-7}$

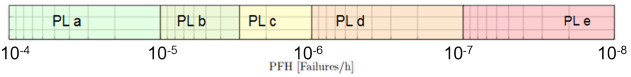

Figure 5 – Graphical representation of table 2

To calculate the PFH, ISO 13849 states that standard's user may calculate it, or use the simplified method presented by the standard. This simplified method consists of estimating some parameters of the safety function, related to the function's architecture, reliability of its components and to detection of failures. These parameters are input to the table K.1 of ISO 13849 (International Organisation for Standardization, 2006), which provides pre-calculated PFH. The process of parameter estimation and determination of PFH according to ISO 13849 is explained in chapter 2.

1.5 LIMITATIONS OF FUNCTIONAL SAFETY

While functional safety is the natural technological development of the safety systems, there are criticism and questions to be answered. The most important questions are explored in this section.

A first question that arises is whether the statistical approach does really make systems safer. There is much effort in determination of PFD_{avg} and PFH, and it is not known whether this effort really reduces accidents in the machinery sector.

Rausand (RAUSAND, 2014) brings a list of open research questions. Among them, software and systematic reliability quantification and estimation of common cause failures stand out as of most importance.

Goble (GOBLE, 2010) brings the question about the quality of reliability methods. Without rational data, calculation methods cannot

deliver meaningful results.

Schaefer and Bork (SCHAERFER; BORK, 2007) recognize that quantification can bring benefits, but has to be regarded skeptically. Users should be able to understand how the reliability numbers of components are produced. Components that are frequently operated are normally subjected to aging and wear failure mechanisms, whereas components that remain long periods inactive are subjected to collapse of tribological system and electrochemical corrosion. Such different failure mechanisms have different failure distributions and parameters.

Due to lack of experienced in safety and reliability, some designers tend to give much importance on the quantification and less importance to safety principles and qualitative requirements. Due to the market pressure, SIL and PL has been seen as a "quality seal", becoming a product feature and a marketing point. Users, seeking only to fulfill numbers, demand for components for functional safety that claim to be "certified". This critic is reinforced by Schaefer and Bork (SCHAERFER; BORK, 2007).

Functional safety are not the only type of safety barrier to be applied, but they are the most complex, demanding more engineering effort. Therefore, there is a false impression that complying to the functional safety standards is enough to achieve a safe system or process.

1.6 RESEARCH AND DEVELOPMENT OF FUNCTIONAL SAFETY

Focus of most of academic research is related to IEC 61508 and IEC 61511. Jin (JIN, 2013) identified the institutes that contribute more to development of functional safety.

One demand of functional safety users, in the field of machine construction, is better understanding of the terms and quantities, and examples of application. In this sense, many companies publish booklets giving overview of requirements, procedures for application of the standard and examples.

In the field of original research and development, there are not many works. Jocelyn (JOCELYN et al., 2014) present an study of application of ISO 13849 in a machine for laboratory use. Focus of the work is to provide an application example and explore variation of parameters for calculation of PFH.

Bosch Rexroth company has taken a position of developer of original research in functional safety for machinery, in the context of

ISO 13849. The first publication is a paper from Orth and Barg (ORTH; BARG, 2010) explaining the impacts of reliability metrics for machine builders. Following this publication, comes the book 10 Steps to Performance Level, in which a methodology for implementation of ISO 13849 is presented, comprising both qualitative and quantitative requirements. Further publications are Orth and Raksch (ORTH; RAKSCH, 2014) for source of reliability data for functional safety, where use of Weibull distribution is suggested to be used when field failure data is available. These publications show that Bosch Rexroth is investing in inclusion of reliability methods in quantification of functional safety, for the machinery building sector.

Other publications of Bosch Rexroth are from Orth, Swagten and Silva (ORTH; SWAGTEN; SILVA, 2014), regarding reliability and functional safety for Oil industrym and from Mikelsons and Su, regarding fault injection simulation with Modelica for validation of functional safety (MIKELSONS; SU, 2014).

1.7 MOTIVATION OF THE PRESENT WORK

For the machinery sector, one of the major issues is the quantification of PFH considering mechanical, pneumatic and hydraulic components. IEC 61508 and IEC 62061 consider only electrical and electronic components, whose times to failure are randomly distributed and well described by the exponential distribution. Referring to figure 4, it represents only **random** failures under component failures. This characteristic allows PFH calculation through homogeneous Markov process, which simplifies the problem.

Pneumatic, hydraulic and electromechanical components exhibit predominantly wear out failure (refer to figure 4). For this reason, the exponential distribution does not represent accurately failures of such components. Weibull distribution is flexible enough to represent well early, random and wear out failures, but does not allow PFH calculation through homogeneous Markov processes.

Table 3 gives a summary of the types of components considered by ISO 13849, as well as their most common reliability measure given by manufacturers. The functional safety assessment framework developed by IEC 61508 does not apply directly in these cases. This problem is cited by Rausand (RAUSAND, 2014) and also by Orth and Raksch (ORTH; RAKSCH, 2014).

[3]Hydraulic valves are also specified in number of cycles for non-safety applica-

Table 3 – Typical reliability measures for common technologies in the machinery sector

Technological group	Reliability measure	Failure distribution
Electrical	Failure rates	Exponential
Electromechanical	Number of cycles to 10% of failure - B_{10}	Weibull
Mechanical	Number of cycles to 10% of failure - B_{10}	Weibull
Pneumatic	Number of cycles to 10% of failure - B_{10}	Weibull
Hydraulic	Mean time to failure[3]	Weibull

The solution used by ISO 13849 is to consider a limited analysis interval and calculate an equivalent constant failure rate for this time interval. This process in described in BGIA Report 2008/2e(HAUKE et al., 2009) and by Schumacher (SCHUMACHER; RüCKWART, 2014). It consists of estimating the frequency of operating cycles, therefrom the time to reach 10% of failed components can be also estimated. A drawback of this approach is that the failure rate has a "expiration date". In order to keep the calculated PFH valid, the component has to be changed after that time, because its failure rate is not valid anymore, regardless if it is still in a good state.

A method for calculation of PFH with Weibull distribution is desired. It relates to the development line of Bosch Rexroth, serving as sequence to the work of Orth and Raksch (ORTH; RAKSCH, 2014) being a further step on the use of Weibull distribution and analysis of field failure data for functional safety.

Detailed calculation models would allow better representation of electromechanical, mechanical, pneumatic and hydraulic systems. It would be possible to investigate effects of slightly variations of architectures.

1.8 OBJECTIVE

The objective of this work is to develop a method that allows calculation of average frequency of dangerous failures per hour (PFH) for typical safety functions in the machinery sector considering components with Weibull distributed failures.

tions. However, ISO 13849 gives standard values for hydraulic components if they fulfill constructive principles.

1.9 METHODOLOGY

This work has been developed in cooperation with Bosch Rexroth AG. The company has a major role in the market of electro-hydraulic components, and it is a leading company in the field of safety and functional safety for machinery sector.

This project includes participation with Bosch Rexroth AG for understanding the current market requirements of functional safety products, as well as the limitations on the techniques available today. Therefore, it is necessary to study the problem, the ways to resolve and to implement it.

Bosch Rexroth aims at improving its processes and products to the Machinery Directive and functional safety. A 6 Degrees-of-Freedom Motion Simulation System was selected to be worked into this process.

As the design office and the design team for motion systems are located in Boxtel, in the Netherlands, as well as a prototype, the project was realized *in loco*. This project is based on the techniques developed in Bosch Rexroth quality department.

The project can be divided in three phases:

1. Study and lectures regarding reliability at the Universidade Federal de Santa Catarina, UFSC;

2. Study of machine safety, functional safety and ISO 13849, and proposal of method with Weibull, developed in Bosch Rexroth Quality Management Department, in Wurzburg, Germany;

3. Project for further development of a motion simulation system with integrated safety functions, in Bosch Rexroth BV, in Boxtel, the Netherlands.

1.10 STRUCTURE OF THE WORK

In chapter 2, the theoretical background of risk, probabilistic risk assessment, risk reduction is given. Additionally to that, reliability measures used for functional safety are given. At the end, some reliability concepts are given.

In chapter 3, a method for considering Weibull distribution for failure of components is developed.

In chapter 4, a case study using the method is given. Results are evaluated in this chapter.

In chapter 5, an integration of the proposed method is made with project activities for compliance to Machinery Directive in a engineering project.

At the end of this work, conclusion and suggestions for future works are presented.

2 FUNCTIONAL SAFETY

As explained in the previous chapter, functional safety reduce inherent risks of technical systems. Safety functions' performance are evaluated by qualitative and quantitative means. In order to enable this evaluation, it is necessary to draw objective measures or framework for quantification of risk and integrity of safety functions.

Much of the quantification techniques of functional safety comes from dependability theory (BUJA; MENIS, 2012). The first section is dedicated to define all the necessary concepts.

A formal definition for risk is given in the second section, as well as a methodology for risk assessment in technical systems. This methodology is used as basis for risk reduction in several industries, including the machinery sector. In the sequence, it is explained how to related reliability/dependability metrics to evaluate the amount of risk reduction of a control system. After that, how this methodology is applied in the machinery sector.

At the end, basic concepts about functional safety are given, necessary to consider for ISO 13849.

Safety and Reliability are knowledge areas that are closely related. There are terms and definitions which are common to both areas, making it difficult to separate them. In the following sections, these terms are defined.

2.1 RELIABILITY ENGINEERING

For the assignment of *performance level, PL* to a safety function, the ISO 13849 requires some qualitative and quantitative measures. The quantitative are expressed in terms of the *average probability of dangerous failures per hour, PFH*. This measure conveys expected lifetime of components, fault tolerance and fault detection, which are part of reliability engineering.

Additionally, as this document focus in application of Weibull distribution for quantification of safety functions, probabilities distributions as exponential and Weibull are presented/explained.

The definitions of quantification follows the approach of Kumamoto(KUMAMOTO; HENLEY, 2000). The symbols used the closest as possible of the one used by IEC 61508-6 and ISO 13849.

Reliability is defined as the ability of an item to perform its

intended function over a period of time under specified conditions (BILLINTON; ALLAN, 1992). The numeric value of reliability means the probability of an item surviving to the given time point.

In order to allow a better and common understanding, some definitions are necessary, and are presented in the following.

Item is a general term meaning the object of the reliability analysis. It covers both system and component.

A **component** is an elementary object of the quantification analysis. It cannot be broken down in parts; it is indivisible. To denote component, sub-index C is used.

A **system** is an item which is a collection (more than one) of components. Quantification analysis of a system depends of the quantification(reliability) of the items, as well as relations between them. To denote system, sub-index S is used.

A **function** is the expected performance of an item. It is expressed in what the item shall deliver, and which variations of performance are acceptable. A **failure** is an event when the system stops delivering the intended function. A failure causes the item to go to a failed state. An item can be either in the normal state, i.e. providing the function, or in the failed state, i.e. not providing the function.

As an example, consider a hydraulic check valve[1], as represented in figure 6. Its function is to allow flow of hydraulic fluid in one direction, and to block flow in the opposite direction. If this valve allows flow in both directions, or if blocks flow in both directions, the valve suffered a failure and is incapable of performing its function.

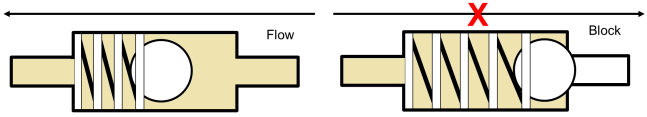

Figure 6 – Schematic representation of a hydraulic check valve.

From the previous definition, it is possible to define **failure mode**. It is the way (mode) in which an item fails. It means how the failure occurs physically (DIAS et al., 2013). Considering the hydraulic check valve, one failure mode is blocking flow in both directions; a second failure mode is to allow flow in both directions.

Dangerous failures are those failure modes can cause harm or impair the machine to react against a dangerous situation. Contrasting

[1] For an electrical counterpart, consider a diode, whose function is to allow electric current in one direction, and to block in the opposite direction.

to **safe failures** that cause the machine not to deliver the intended function, but do not pose hazards. Safe and dangerous failures are further explored in section 2.2.

A **Repairable** item means that after a failure, the same item can deliver the intended function after a **maintenance** action, also called **repair**.

A **Non-repairable** item means that it cannot deliver the function anymore, even after a maintenance action. The item has to be discarded and replaced. In this work, systems are considered repairable items, while components are considered non-repairable items. A representation of repairable and non-repairable items is given in figure 7.

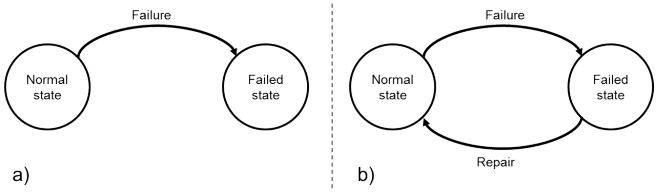

Figure 7 – Model for a a) non-repairable and b) repairable item.

Component reliability and system reliability configure two difference study areas. The first one is concerned with the physical mechanisms of failures, how to determine the reliability through laboratory life tests or analysis of field failures and design modification to optimize reliability of a component. System reliability is concerned with quantification the reliability metrics of a system, allocation of components to achieve a reliability goal, and to understand the relation between them.

Reliability engineering is based on probability theory and random variables. In the following sections, some concepts of reliability engineering are detailed, in order to allow definition of evaluation metrics for functional safety. The random variable T denotes lifetime.

2.1.1 Cumulative Distribution Function

Is the probability of failure until a time t. In mathematical terms, it is the probability that the random variable T is lower than t. (That is, probability that a value for lifetime of an item chose at random is lower than the limit t). It is denoted by $F(t)$, and calculated

by (BILLINTON; ALLAN, 1992):

$$F(t) = P\{T < t\} \tag{2.1}$$

Where P stands for probability.

2.1.2 Survival Function

Is the probability of an item to perform its function (without failing) until the time t[2]. It is denoted as $R(t)$, called **Reliability Function**, expressed by (BILLINTON; ALLAN, 1992):

$$R(t) = P\{T > t\} \tag{2.2}$$

2.1.3 Probability Density Function

The concept of *probability density function, PDF* expresses the instantaneous behavior of the probability. It is the quantification of the failures by each time instant, normalized by the initial population. It can be thought as the probability of failure per unit of time. The *pdf* is denoted by $f(t)$ and is calculated by (BILLINTON; ALLAN, 1992):

$$f(t) = \frac{dF(t)}{dt} \tag{2.3}$$

2.1.4 Failure rate

Failure rate[3]is one the most used reliability indicators (BILLINTON; ALLAN, 1992).It is the number of items that will fail in the next time instant $[t, t + dt)$, given the number of items that have not failed until time instant t. It is normally denoted by the Greek letter λ and calculated by (BILLINTON; ALLAN, 1992):

$$\lambda(t) = \frac{N(t + dt) - N(t)}{N_{survived}(t)} \tag{2.4}$$

[2]Mathematically, it is the probability that a value for lifetime T of an item picked at random is higher than t.

[3]Some authors call this quantity by *hazard rate* or *hazard function*. This name is avoided in this work, as it may cause confusion.

Where $N(t)$ stands for number of failures at time instant t and $N_{survived}(t)$ stands for number of items working at time instant t.

Alternatively, it can be calculated by the reliability function and the *pdf*, as (RIGDON; BASU, 2000):

$$\lambda(t) = \frac{f(t)}{R(t)} \tag{2.5}$$

Formally speaking, the failure rate is a conditional quantity. That is, it is conditioned that the components have not failed until the time point t of interest. However, due to the disseminated use of the name *failure rate*, it is maintain in this document, without the *conditional*.

2.1.4.1 Failure rate curve

The failure rate expresses a very important characteristic of items. A plot of failure rate of items of its life shows a specific pattern[4]. It can be seen in figure 8. This represents a initial phase of life where components are much more prone to failure, due to weak design, production flaws and assembly errors. Following that, there is a flat region, where the failure rate is approximately constant, that accounts for random failures, caused by random and unknown factors. At the end, the item enters in a wear-out phase, where aging mechanisms start to take effect and accumulated damaged start to make components fail more.

This representation of different failure mechanisms is included in figure 4.

2.1.5 Mean time to failure - MTTF

The Mean Time To Failure is a widely used concept in reliability. Mathematically, it is defined as the expected value of the lifetime T, and calculated by the equation:

$$MTTF = E(T) = \int_0^\infty t f(t) dt = \int_0^\infty R(t) dt \tag{2.6}$$

The equation 2.6 applies to every distribution. However, MTTF

[4]The failure rate curve is often referred as hazard rate curve or bathtub curve.

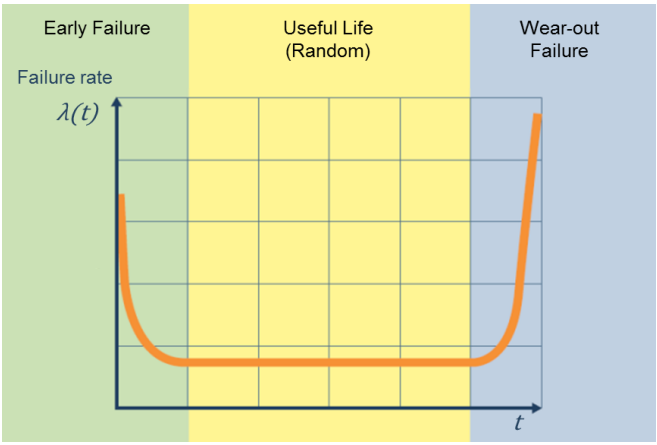

Figure 8 – Theoretical model of failure rate through the lifetime

has adopted a specific meaning in reliability engineering.

For the exponential distribution (see section 2.1.9), the failure rate becomes constant, and it can be shown that MTTF equals the inverse of the failure rate, as shown:

$$MTTF = \frac{1}{\lambda} \tag{2.7}$$

Where λ stands for a constant failure rate.

Considering the bathtub curve, the middle region, called useful life, can be modeled by the exponential distribution. In that sense, it has been conventionalized that MTTF represents the inverse of the failure rate during the useful life. In this case, it can assume very high values (low failure rates), but once the item reaches the end of its useful life and enters in the wear-out phase, the assumed value for MTTF is not valid anymore.

2.1.6 B_X% life

For components whose failures are mainly due to time- and use-dependent failure modes, it is common to express reliability (or lifetime) in terms of time to a certain percentage of failure.

This measure is denoted by B_X, where X is replaced by the percentage. In that way, B_1 means 1%, B_5 means 5%, B_{10}, 10% and

so on.

For discrete components, i.e. components that operation is characterized by two distinct states (e.g. open and closed) as pneumatic valves and electromechanical switches, reliability is commonly measured in B_{10} cycles. This is interpreted as the number of cycles until 10% of the components have failed in life tests.

The B_{10} is mainly used for components operate in cycles. For other components, whose operation is rather continuous, like bearings, it is common to refer to L_{10}, measured in (continuous) operating hours.

2.1.7 Unconditional failure intensity

The unconditional failure intensity, normally denoted by $w(t)$, is calculated by the number of items that will fail within the small interval $[t, t + dt)$, given that the components were working at the beginning of the test. It is calculated as:

$$w(t) = \frac{N(t, t + dt)}{N_0} \tag{2.8}$$

Where N_0 is the number of items in normal condition at t = 0.

As this measure considers the whole population, even the failed items, it becomes the same as the probability density function (pdf) for non-repairable components. For repairable, it does not equal to the probability density function nor to the failure rate.

2.1.7.1 Difference between failure rate and unconditional failure intensity

Failure rate and unconditional failure intensity are normally confused. In order to clarify these concepts, and the difference between them, consider example in figure 9.

The failure rate $\lambda(t)$ is calculated using equation 2.4, considering only the items that have not failed until the time t:

$$\lambda(t) = \frac{7}{70} = 0.1 \tag{2.9}$$

While the unconditional failure intensity $w(t)$ is calculated using equa-

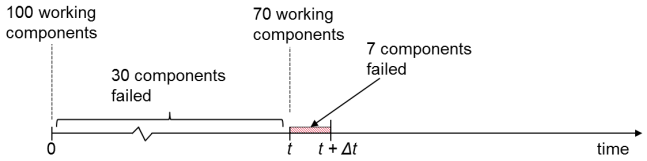

Figure 9 – Failure rate versus unconditional failure intensity. Adapted from Kumamoto (KUMAMOTO; HENLEY, 2000). Time axis is not in scale.

tion 2.8, considering the initial amount of items:

$$w(t) = \frac{7}{100} = 0.07 \tag{2.10}$$

2.1.8 Component reliability - Failure distributions

The component reliability is concerned in quantify the failures of a single component. Reasons for that is to optimize design of a component. The analysis is done mostly in the structural level, looking at the physics of the failure. Objective is to understand how a particular failure mode occurs, and to change the design to avoid such failures (or even to avoid over-design).

2.1.9 Lifetime distributions - Exponential

The exponential distribution is the
The probability density function becomes:

$$f(t) = \begin{cases} \lambda e^{-t\lambda}, & t > 0,\ \lambda > 0 \quad (2.11a) \\ 0, & \text{otherwise} \quad (2.11b) \end{cases}$$

The cumulative failure distribution becomes:

$$F(t) = 1 - e^{-t\lambda} \tag{2.12}$$

The reliability distribution becomes:

$$R(t) = e^{-t\lambda} \tag{2.13}$$

The failure rate becomes:

$$\lambda(t) = \lambda \tag{2.14}$$

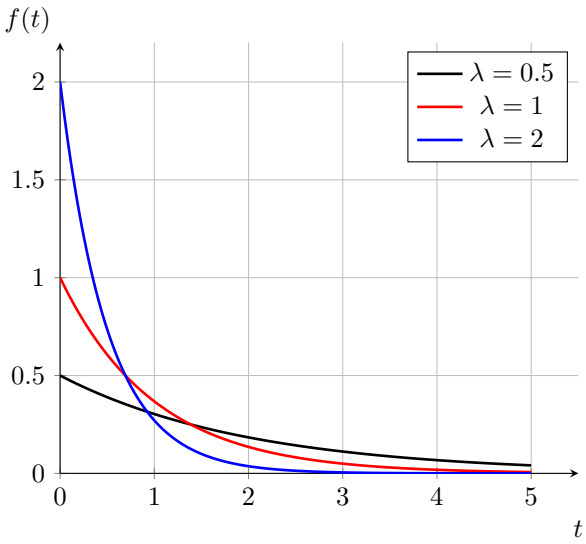

Figure 10 – Probability Density Function of the Exponential distribution

2.1.10 Lifetime distributions - Weibull

The Weibull distribution is characterized by having no typical shape. Its shape is defined by its parameters. Weibull distribution is found in two forms: two-parametric and three-parametric. The three-parametric distribution represents an additional lifetime with no failures, and it is of no interest for this work, therefore will not be considered. The two-parametric Weibull distribution has the parameters:

- Scale parameter, denoted here by η; and
- Shape parameter, denoted here by β.

The η parameter represents lifetime of an item. The higher the η value, the longer the duration of an item. The β parameter represents

whether failures tend to occur in the beginning, middle or the end of lifetime. Failure rate of the Weibull distribution can represent each of the three regions of the failure rate curve (refer to figure 8) and therefore the three failure mechanisms of figure 4.

Due to its flexibility, the Weibull distribution is well-suited for shape fitting applications, and therefore it is used for analysis of field failures. The probability density function becomes:

$$f(t) = \begin{cases} \frac{\beta}{\eta}(\frac{t}{\eta})^{(\beta-1)} e^{-(\frac{t}{\eta})^{\beta}}, & t > 0 \quad (2.15a) \\ 0, & \text{otherwise} \quad (2.15b) \end{cases}$$

The cumulative failure distribution becomes:

$$F(t) = 1 - e^{-(\frac{t}{\eta})^{\beta}} \tag{2.16}$$

The reliability distribution becomes:

$$R(t) = e^{-(\frac{t}{\eta})^{\beta}} \tag{2.17}$$

The failure rate becomes:

$$\lambda(t) = \beta(\frac{1}{\eta})^{\beta} t^{\beta-1} \tag{2.18}$$

2.1.11 Availability

Defined only for repairable items. It is the probability of an item is normal at time t. It is denoted by $A(t)$, and calculated by (KUMAMOTO; HENLEY, 2000):

$$A(t) = P\{Item\ is\ working\ at\ t\} \tag{2.19}$$

2.1.12 Unavailability

As availability, it is also defined only for repairable items. It is the probability of an item is failed at time t. It is denoted by $Q(t)$, and calculated by (KUMAMOTO; HENLEY, 2000):

$$Q(t) = P\{Item\ is\ not\ working\ at\ time\ t\} \tag{2.20}$$

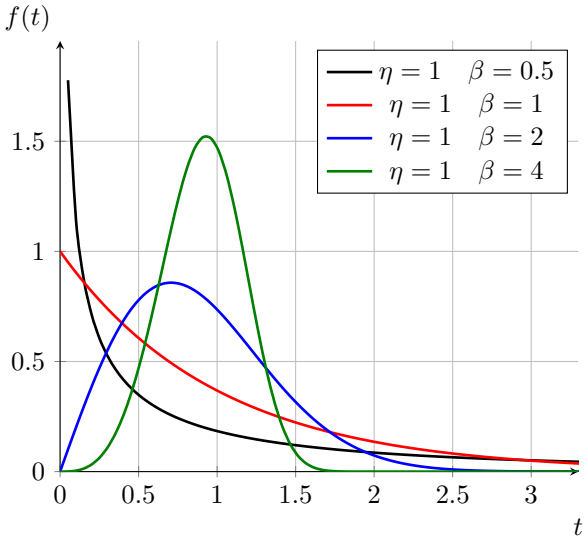

Figure 11 – Probability Density Function of the Weibull distribution

2.1.13 Repair rate

Repair rate is an analogous quantity as failure rate, but defined for components that are failed and are repaired. Formally, it is the probability that an item is repaired in the interval $[t, t + dt)$, given it is failed at t (KUMAMOTO; HENLEY, 2000). It is denoted by function $\mu(t)$.

2.1.13.1 Mean Time To Repair - MTTR

As the MTTF, the Mean Time To Repair - MTTR, is the expected value of time to repair (KUMAMOTO; HENLEY, 2000)

For constant repair rate, i.e. $\mu(t) = \mu$, the relation is valid:

$$MTTR = \frac{1}{\mu} \tag{2.21}$$

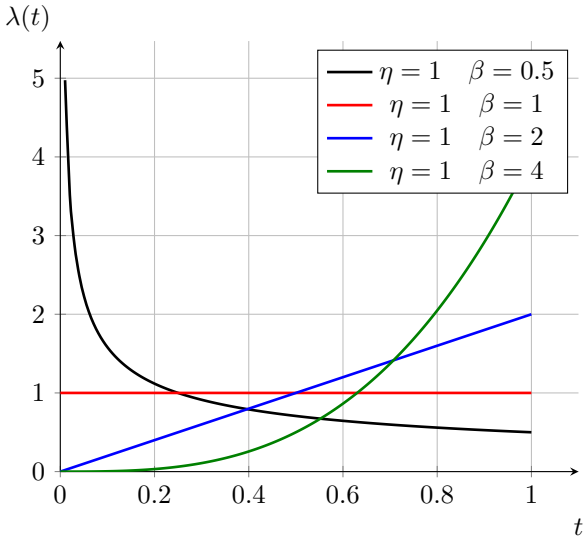

Figure 12 – Failure rate of the Weibull distribution

2.1.14 System reliability

System reliability has two objectives: quantify the reliability metrics of a system, based on the values/figures of components, and to understand the relation between them.

The problem of system reliability is the one of modeling a complex engineering with a lot of components and their interactions between them. The objective of system reliability is to provide an answer about the behavior of a system (beforehand) given the behavior (reliability) of the components. Many other analysis come from that, like analysis of importance of components, reliability allocation and so on.

2.1.15 Series and parallel configuration

Reliability modeling does not correspond necessarily with the physical structure of a system. Reliability modeling takes the function into account, and what are the components that contribute to the function. In that way, it becomes important to have a precise definition of function.

When two (or more) components are necessary for a function, they are modeled as in **series** configuration. Figure 13 shows a representation of series system. If one of them fails, the complete system fails.

$$R_S(t) = R_A(t) \cdot R_B(t) \tag{2.22}$$

Where $R_S(t)$, $R_A(t)$ and $R_B(t)$ denotes the reliability function for the system, component A and component B, respectively.

Figure 13 – Block diagram of a series system with two blocks

If two components realize the same function, and failure of one is not enough to make the system fail, they are said to be **redundant** and the system has a **parallel** configuration. Figure 14 shows a representation of a parallel configuration. In this case, the reliability of the system, based in the reliability of the components is given by:

$$R_S(t) = R_A(t) + R_B(t) - R_A(t) \cdot R_B(t) \tag{2.23}$$

Each chain of components realizing the function is called a **channel**. A series configuration is also referred as a **single channel** structure, while a **dual channel** structure means a parallel configuration.

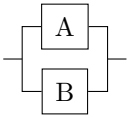

Figure 14 – Block diagram of a parallel system with two blocks

Series systems have lower reliability than its components, while parallel systems have higher reliability. If one of the components fail in a redundant structure fail, the second can still provide the function. The failures that affect one component do not affect the other, therefore increasing the reliability of the system.

2.1.16 Common Cause Failures - CCF

Usage of redundant components may improve the reliability of a system, without having to increase the reliability of the component itself. In the case of a failure of a component, the other one can still deliver the function. This is due to the fact that failures are independent and that causes of failure of one component do not cause the other to fail. However, if the component are similar or equal to each other, they are prone to fail due to same causes and/or stresses. This effect reduces the gain in reliability when redundant structures are used.

Failures of redundant structures due to same causes are called common cause failures - CCF, and modeling of such failures is important to give a more realistic and not so optimistic reliability estimation (BILLINTON; ALLAN, 1992).

2.1.16.1 Beta-factor model

The Beta-factor model divides the failure rate of each component of a parallel structure into common-cause failure rate (two components fail) and single failure rate (one component fails). This division is made considering a multiplicative factor, called β_{CCF} (GOBLE, 2010). It assumes a value between 0 and 1, normally lower than 0.1 (lower than 10%) (DORRA; REINERT, 2000).

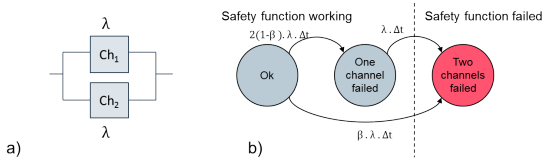

Figure 15 – Representation of common cause failures with Beta-factor

Figure 15 a) represents a parallel structure with two equal blocks. Each block has failure rate λ. Figure 15 b) a state transition diagram of failure as figure 7, but considering two components in parallel structure. If one fails, safety function is still provided by the second, what is represented as the transition from “Ok” to “One channel failed” state. However, a failure due CCF means a transition directly from state “Ok” to “Two channels failed”, and the second component did have no effect in increasing reliability of the system. Consideration of CCF adjusts

failure rates for:

$$\lambda_{noCCF} = \lambda \cdot (1 - \beta_{CCF}) \tag{2.24}$$

While both blocks fail at the same time with failure rate:

$$\lambda_{CCF} = \lambda \cdot \beta_{CCF} \tag{2.25}$$

2.1.17 Modeling and quantification of system reliability

There are different techniques for representing reliability of a system, based on reliability of its components. Each modeling technique has different properties; some focus more on the relation of components itself, some on the system behavior. According to IEC 61508-6 (International Electrotechnical Comission, 2010b), the more common techniques are:

- *Reliability Block Diagram - RBD*;
- *Fault Tree Analysis - FTA*;
- Markov process;
- Monte Carlo simulation;
- Discrete Event simulation;
- *Generalized Stochastic Petri Nets - GSPN.*

There are plenty of literature about calculation of PFH with each method and comparison between them. One of the most important is the Annex B of IEC 61508 part 6 (International Electrotechnical Comission, 2010b), which summarizes how to calculate PFD and PFH with RBD, FTA, Markov process, Monte Carlo and other techniques. For a comparison between all method, refer to the work of Rouvroye (ROUVROYE; BLIECK, 2002). For an explanation of how to calculate PFH with FTA, Markov process and GSPN, refer to the work of Inal et al (INNAL et al., 2010). Rausand (RAUSAND, 2014) has a good compilation of calculation with different techniques.

2.2.1 Risk

Risk is a concept associated with potential loss (or gain) of an uncertain event. It is denoted by R and is calculated by:

$$R = S \cdot P \tag{2.26}$$

Where S stands for severity and P for probability of occurrence.

2.2.2 Ratio of dangerous failure

While in reliability engineering all the failures are a matter of concern, in safety engineering only dangerous failure modes are of concern.

Therefore, failure rates or MTTF must be corrected by a factor, called ratio of dangerous failures. This factor is estimated by a Failure Modes and Effects Analysis (FMEA), considering which failure modes are dangerous for the system.

For ISO 13849, when no information regarding ratio of dangerous failure is provided, it shall be considered as 50%.

2.2.3 Mission time

Mission time is the maximum allowed time for the safety-related control system to operate. It is denoted as T_M.

2.2.4 Average frequency of dangerous failure per hour - PFH

For safety standards, it is necessary to estimate PFH. It means average frequency of dangerous failure per hour, and it is a characteristic of a system, which depends, among other things, on the quality of its components, the architecture, detection of failures and repair. For an intuitive interpretation of PFH, see appendix B. It is defined by the

IEC 61508-4 (International Electrotechnical Comission, 2010a) as:

$$PFH(T_M) = \frac{1}{T_M} \int_0^{T_M} w_S(t)dt \tag{2.27}$$

Where $PFH(T_M)$ is the average frequency of dangerous failure over the interval $[0, T_M)$, T_M is the mission time and $w_S(t)$ is the unconditional failure intensity of the complete safety function (system).

Estimation of $w_S(t)$ is done differently for each system reliability method listed in section 2.1.17. Innal et al. (INNAL et al., 2010) explains how to calculate PFH using FTA, Markov models and GSPN. For this work, PFH is estimated by discrete event simulation. A deeper explanation is given in section 3.4.

The PFH can be estimated by the average number of failures, divided per time according to IEC 61508-6 (International Electrotechnical Comission, 2010b). For Kumamoto (KUMAMOTO; HENLEY, 2000), the expected number of failures is the integral over time of the unconditional failure intensity, as given:

$$E(N(T_M)) = \int_0^{T_M} w_S(t)dt \tag{2.28}$$

where $E(N(T_M))$ is the expected value of the number of failures in the interval $[0, T_M)$. Algebraic manipulation of equations 2.27 and 2.28 leads to:

$$PFH(T_M) = \frac{1}{T_M} E(N(T_M)) \tag{2.29}$$

With simulation, it is possible to calculate the average number of failures, which is an estimate for the expected number of failures. Therefore, equation 2.29 is used to calculate PFH.

2.3 FUNCTIONAL SAFETY FOR INDUSTRIAL MACHINERY - THE ISO 13849

Many hazards arise from an improper behavior of the machine and its moving parts. This behavior is controlled by the control system. It is therefore necessary that the control system is properly designed, in order to avoid such hazards. Safeguarding measures cannot block the complete access to the hazardous parts of the machine (most of the time, access should be granted for maintenance purposes). In these

cases, it is necessary that safeguards can trigger the machine to go to a safe state or have a safe behavior.

Typical safety function for the machinery sector defined by ISO 13849 (International Organisation for Standardization, 2006):

- Safety-related stop initiated by a safeguard;
- Manual reset function
- Start/restart function
- Enabling device function
- Prevention of unexpected start-up
- Escape and rescue of trapped persons

A safeguard, when properly designed, would remove the possibility of an accident to occur. However, due to complexity of the matter, it is virtually impossible to consider all the cases and to ensure that the control system has no design flaws. Nevertheless, it is also subjected to failure of components.

If a component fails, the safety function is not available anymore and an accident can occur due to an exposed hazard.

The simplified method for quantification of PFH for the machinery sector relies in determining 3 parameters: category, MTTF_d and DC_{avg}.

2.3.1 Categories

Category is a basic requirement for compliance to the standard. Every safety function must be classified into a category, in order to be assigned to a PL.

The category concept conveys the behavior of the function in the event of a failure. It is strongly related to the structure of the function, i.e. how the components are relate to each other. As there are many possible structure variations, the standard described them in abstract terms, so that a great variety of structure can be mapped into few categories (International Organisation for Standardization, 2006).

Each category is represented in the standard by a **designated architecture**. A designated architecture is a typical implementation in block diagram that fulfills the requirements of each category. They

should be considered a guide to the implementation, but not only the unique solution to each category.

Each category requires an interval of values of $MTTF_d$ and DC_{avg}. Categories 2, 3 and 4, which have redundant channels, have to fulfill additional requirements against common cause failures[5], called CCF for short.

2.3.1.1 Category B

This category is characterized by design of the safety function according to relevant standards to the application and to withstand operational stresses, influence of processed materials and environmental conditions.

A failure of any component may cause the failure of the safety function. A safety-related block diagram[6]of designated architecture for category B is shown in figure 16.

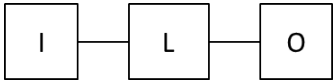

Figure 16 – Graphical representation of designated architecture for category B and 1. I stands for Input element, L for Logic and O for output element.

Category B and its designated architecture (figure 16) can be seen as a technical implementation of the behavior of figure 3. An example for a category B safety function is an interlock sensor in a door of a machining center, triggering a signal when to a PLC when the door is opened, which disables a power contactor relay. A dangerous failure in any element causes the safety function to fail.

[5]Proportion of failures due to common cause is not directly estimated by the user in ISO 13849. A proportion of 2% was assumed by the standard committee, which has to be assured if enough measures are taken. The user has implement some of the measures, which are listed in Annex F of ISO 13849-1.

[6]Safety-related diagram block is a graphical representation introduced by ISO 13849. This representation resembles Reliability Diagram Blocks (RBD), but there are not equivalent. Safety-related block diagrams are intended only for representation purposes, not for quantification.

2.3.1.2 Category 1

This category is based in the category B, with the addition that only components that are proven to be suitable to safety application, either by use in the past or suitable verification. Programmable components are not allowed for category 1. A safety-related block diagram of designated architecture for category 1 is shown in figure 16.

2.3.1.3 Category 2

Additionally to the requirements of category B, category 2 requires that the correct operation of the safety function must be monitored. In the case of a failure that can be detected, the SRP/CS must trigger a reaction, which can be either signalizing the fault or bringing the machine to a safe condition. A safety-related block diagram of designated architecture for category 2 is shown in figure 17.

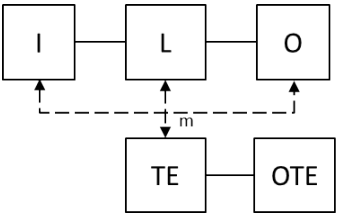

Figure 17 – Graphical representation of designated architecture for category 2. I stands for Input element, L for Logic, O for output element, m for monitoring, TE for test equipment and OTE for Output of the test equipment.

A typical example for a category 2 system is use of a watchdog module for verification of software execution. In case of an error, watchdog module triggers an error signal.

2.3.1.4 Category 3

A category 3 function must fulfill the requirements of category B and, as main characteristic, a single fault of any component does not cause the failure of the safety function. It represents usage of redundancy in the safety function, which must comply to measures to

avoid common cause failures. Failures of components must be detected to a reasonable effort. A safety-related block diagram of designated architecture for category 3 is shown in figure 18.

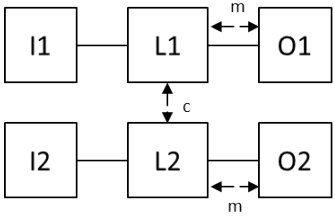

Figure 18 – Graphical representation of designated architecture for category 2. I1 and I2 stands for Input, L1 and L2 for Logic, O1 and O2 for output element, m for monitoring and c for cross-monitoring.

2.3.1.5 Category 4

For compliance with category 4, a function must provide tolerance at least against one component failure, and failures must be detected before a next demand arises. If a failure is undetectable, then an accumulation of failures shall not cause the failure of the function. A safety-related block diagram of designated architecture for category 4 is shown in figure 19.

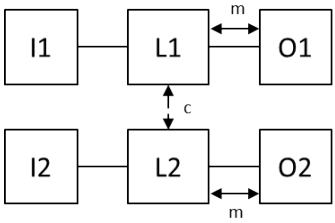

Figure 19 – Graphical representation of designated architecture for category 2. I1 and I2 stands for Input, L1 and L2 for Logic, O1 and O2 for output element, m for monitoring and c for cross-monitoring. Difference from figure 18 are the solid lines between L and O, denoting intensive monitoring.

2.3.1.6 Custom architectures

ISO 13849 requires that architectures of safety functions be assigned to a category. This is a normative requirement[7] for assignment of PL. **Designated architectures** are used to graphically represent the categories, and were used to calculate values of table K.1. However, the standard states that custom architectures may be used as well, as long as they are shown to be equivalent.

Categories specify desired *behaviors* of the safety function in the case of a failure, not a specific architecture. So, if different implementation achieve the same behavior, they may be claimed as the same category. For example:

- A safety function implemented with three-channels may be regarded as category 3 or 4, depending on other characteristics. If some failures are detected, it can be regarded as category 3. If detection of failures is improved, it may achieve category 4[8];
- A safety function with two channels, but no diagnostics, may be regarded as category B or 1.

2.3.2 Mean Time to Dangerous Failure - $MTTF_d$

For ISO 13849, reliability of components and safety functions are quantified in terms of the Mean Time To *dangerous* Failure, $MTTF_d$.

The $MTTF_d$ is the inverse of failure rate (see section 2.1.5), considering only dangerous failure modes. To calculate it, it shall be considered the ratio of dangerous failures (refer to section 2.2.2). For some components, manufacturers state the $MTTF_d$ value, and what are the dangerous failure modes considered. In other cases, it must be specified from the Ratio of dangerous failures, calculated by a Failure Mode and Effects Analysis (FMEA). If neither is possible, ISO 13849 state that 50% of all failures must be considered dangerous, as a conservative approach.

From the $MTTF_d$ of components, it is necessary to estimate an $MTTF_d$ for the complete safety function. The process for estimation of the safety function $MTTF_d$ is as follows:

[7] mandatory

[8] Further investigation on models for quantification of common cause failures would still be necessary.

1. Evaluate the MTTF_d of each component;
2. Estimate the MTTF_d of each channel using parts count method;
3. Calculate an equivalent MTTF_d from both channels with equation 2.31 .

For evaluation of MTTF_d of each component, different data sources may be used. Preferred are data from manufacturers.

For estimation of the MTTF_d of each channel, it is necessary that the structure of the function is already known. Therefrom is possible to know to whichever channel each component belongs, and combine them for each channel through the equation:

$$\frac{1}{MTTF_d} = \sum_{i=1}^{N} \frac{1}{MTTF_{di}} \tag{2.30}$$

In the case of redundant structures (categories 3 and 4), there is an MTTF_d for each channel, which may be different from each other. In this case, it is necessary to calculate an equivalent MTTF_d, through the equation:

$$MTTF_d = \frac{2}{3}\left[MTTF_{d,C1} + MTTF_{d,C2} - \frac{1}{\frac{1}{MTTF_{d,C1}} + \frac{1}{MTTF_{d,C2}}}\right] \tag{2.31}$$

Resulting MTTF_d value can be then used in the table K.1 from ISO 13849.

The standard limits MTTF_d of each channel between 3 and 100 years. An MTTF_d lower than 3 years is not allowed; higher than 100 years is considered as 100 years. Components are allowed to have higher MTTF_d.

MTTF_d shall not be considered as a measure of lifetime; it must be considered strictly as a failure rate valid within a time frame and under specified conditions. An MTTF_d of 3 years do not mean that a component lasts for 3 years neither that it is the minimum mission time; it means that the considered failure rate is:

$$\lambda_d = \frac{1}{MTTF_d} = \frac{1}{3\,years \cdot 8670\,hours/year} = 3.81{\cdot}10^{-5} failures/hour \tag{2.32}$$

Limitation in range of allowed MTTF_d values can be interpreted as limitation in the range of allowed failure rates. g In the sense of ISO

Table 4 – DC_{avg} classification

Denotation	Range
None	$DC_{avg} \leq 60\%$
Low	$60\% < DC_{avg} \leq 90\%$
Medium	$90\% < DC_{avg} \leq 99\%$
High	$99\% < DC_{avg}$

13849, as an $MTTF_d$ for pneumatic, hydraulic and electromechanical components is calculated from B_{10} values, a limit for utilization of obtained $MTTF_d$ must be calculated. If this limit is inferior to mission time T_M, the component has to be changed after the limit has expired.

2.3.3 Average Diagnostic Coverage - DC_{avg}

The diagnostic coverage is the proportion of the failures of a component which can be detect through testing and monitoring. This value is dependent of the system configuration and measures adopted by the machine designer. Strictly speaking, diagnostic coverage is calculated by:

$$DC = \frac{\sum \lambda_{d,D}}{\sum \lambda_d} \tag{2.33}$$

Where $\lambda_{d,D}$ is the failure rate of the *dangerous* failure modes which are detected and λ_d is the failure rate of all *dangerous* failure modes.

As normally the designer does not have detailed information regarding failure rates and failure modes, ISO 13849 list some common failure detection measures for different components and technologies, with typical DC values, in Annex E. In that way, DC of each component can be estimated by the measures implemented in the machine.

The average diagnostic coverage DC_{avg} is a weighted average of the DC of all components. The weighting factor is the MTTFd of each component. It is estimated by:

$$DC_{avg} = \frac{\frac{DC_1}{MTTF_{d1}} + \frac{DC_2}{MTTF_{d2}} + \cdots + \frac{DC_N}{MTTF_{dN}}}{\frac{1}{MTTF_{d1}} + \frac{1}{MTTF_{d2}} + \cdots + \frac{1}{MTTF_{dN}}} \tag{2.34}$$

In order to have a table with reduced size, DC_{avg} s classified into four levels, as represented in table 4.

The resulting categorized DC_{avg} value can be then used in the

table K.1 from ISO 13849.

With category, MTTF_d and DC_{avg}, PFH can be estimated by table K.1 from ISO 13849. Figure 20 is a summary of the table, and provides an overview of which PL is possible to reach with each category.

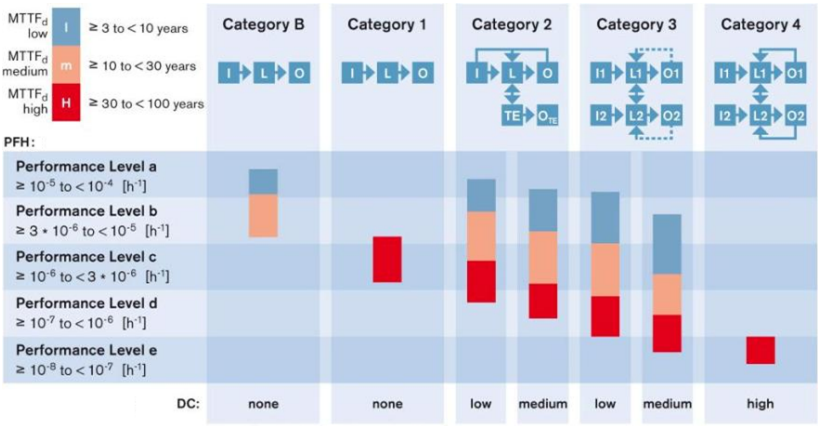

Figure 20 – Summary of table K.1 of ISO 13849. Reproduced from Bosch Rexroth (ORTH et al., 2012)

The ISO 13849 standard gives guidance only for PFH estimation with table K.1 and the bar chart (see figure 20). There is no guidance on how to build models, nor how to evaluate it. In the next chapter, methods for PFH estimation are developed and verified against table K.1

3 ALTERNATIVE METHODS FOR PFH CALCULATION

The ISO 13849 standard can be seen as a method for the *average frequency of dangerous failure per hour, PFH* estimation, given category, MTTF_d and DC_{avg}. This method consists of a table for some common cases in the machinery sector. This is represented in figure 21, a). This method is however a black box. There is no documentation of how these values presented in the table K.1 from ISO 13849 were calculated in details. There is only the STSARCES Report (DORRA; REINERT, 2000), which was an investigative report that gave the basis for ISO 13849.

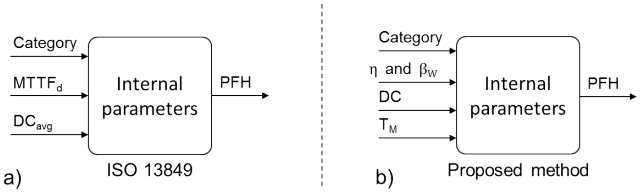

Figure 21 – Differences between current method by a) ISO 13849 and b) proposed method. In b), instead of specifying MTTF_d for the safety function, it is necessary to specify the parameters of Weibull distribution, η and β_W. It is also necessary to specify mission time T_M.

The objective of this chapter is to present a method for calculation of redundant architectures with components whose failures follow the Weibull distribution, as represented in figure 21, b).

3.1 HOW WAS CONSTRUCTED TABLE K.1 OF ISO 13849?

Models for PFH calculation can include more or less details (GOBLE, 2010), depending of what is intended with the analysis. For each category of ISO 13849, a Markov model was generated to represent its correspondent designated architecture (see sections 2.3.1.1 to 2.3.1.5), including failure rates of each block individually, frequency of automatic tests performed by the system to detect failures, diagnostic coverage, time to repair of the safety system, rate of demands of safety function, proportion of failures due to common causes, among others. It is not know how detailed and which parameters were considered as

the results were grouped into ranges of $MTTF_d$ and DC_{avg}.

STSARCES Report (DORRA; REINERT, 2000) was an investigation report that applied Markov process to model categories of EN 954[1]. Models were constructed considering the whole safety function at once, i.e. all functional blocks (Input, Logic, Output). This approach generates big and complex models, once number of states in a Markov model increases exponentially with the number of blocks, but it was preferred in order to evaluate the influence of each individual parameter in the model. Table K.1 of ISO 13849 was generated from such models, taking mean values of exhaustive test calculations.

Studies of the German Institute for Insurance against Work Accidents (HAUKE et al., 2009, pp. 348) state that the absolute value of demand and test rate have a negligible effect on the PFH. Main influence is exerted by the overall failure rate, represented by $MTTF_d$, by diagnostic coverage DC_{avg} and by the structure.

Other parameters beyond those explicit in table K.1 a were modeled. As influence of their variation is small, they were considered internally in the calculation models, but not made explicit. They are:

- Demand rate
- Frequency of tests
- Repair rate or Repair time
- Proportion of Common Cause Failures
- Mission time[2]

Even that the exact model that generate the table K.1 is not known, it is useful to know the modeling process and hypotheses used, in order to be able to transfer to another modeling technique. It has to be then evaluated which of the hypothesis and details can be modeled or ignored in the new techniques.

3.2 PFH CALCULATION BY DISCRETE EVENT SIMULATION

For this problem, safety functions are modeled in Reliability Block Diagrams, RBD for short, and PFH is evaluated by discrete event

[1] EN 954 is the predecessor standard for safety of machine controls. See section 1.4.1 and Lereverend(LERéVéREND, 2008).

[2] Considered as a limit for the utilization of the component

simulation. This technique is preferred because the reliability representation is close to schematic drawings and physical components, facilitating comprehension of technicians and engineers that do not have knowledge in reliability modeling. Use of simulation allows calculation of PFH considering any failure distribution, inclusive Weibull distribution.

Basis of calculation is explained by mean of an example. In figure 23, PFH is obtained by simulation. A reliability block diagram (RBD) is modeled as in figure 22. In this model, block A represents failures in channel 1 that are detected, block B represents failures in channel 1 that are undetected, block C represents failures in channel 2 that are detected, block D represents failures in channel 2 that are undetected and block E represents failures due to common causes (CCF).

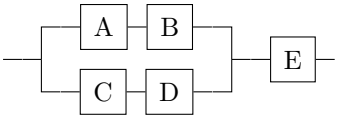

Figure 22 – 1oo2 RDB for category 3 or 4. Block A represents detected failures in channel 1; block B, undetected failures in channel 1; block C, detected failures in channel 2; block D, undetected failures in channel 2 and block E, failures due to common causes (CCF).

Figure 23 represents dynamics of reliability simulation, i.e. events during simulation time. All component failures considered in this example are dangerous. It is important to notice that not every dangerous component failure leads to a dangerous control system failure. Effects of failures on the safety system are discussed as follows.

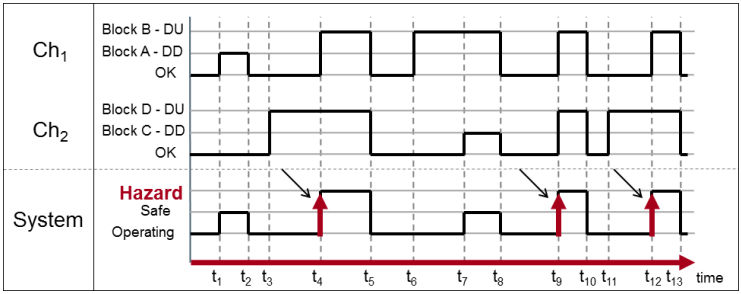

Figure 23 – Simulation for determination of PFH. Time axis is not intended to be in scale and do not represent typical values.

1. At time t_1, a component in channel 1 fails, but it is detected by the control system. Machine goes to a safe state. Operation is stopped, but there is no hazardous situation due to the control system;

2. At time t_2, the failed component is repaired. The machine returns to operation;

3. At time t_3, a component in channel 2 fails and it is not detected by the control system. Machine continues to operate, and it is still safe because safety function is still provided by channel 1;

4. At time t_4, a component in channel 1 fails and it is not detected by the control system. Machine continues to operate, but in a hazardous condition, as the safety function is not provided anymore;

5. At time t_5, a demand on the safety function reveals that it is not being provided. Machine has to be stopped and components have to be repaired. After repair, machine continues to operate;

6. At time t_6, a component in channel 1 fails and it is not detected by the control system. Machine continues to operate, and safety function is still provided by channel 2;

7. At time t_7, a component in channel 2 fails, but it is detected by the control system. Machine goes to a safe state;

8. At time t_8, components of both channels are repaired and machine returns to operation. Safety function is restored;

9. At time t_9, components of both channels fail due to a common cause, represented by block E of figure figure 22. Machine continues to operate, but in a hazardous condition, as the safety function is not provided anymore;

10. At time t_{10} a demand of the safety function reveals that it is not being provided. Components are repaired and machine returns to operation;

11. At time t_{11}, a component in channel 2 fails and is not detected by the control system. Machine continues to operate and safety function is still provided by channel 1;

12. At time t_{12}, a component in channel 1 fails and is not detected by the control system. Machine continues to operate, but in a hazardous condition, as the safety function is not provided anymore;

13. At time t_{13} a demand of the safety function reveals that it is not being provided. Components are repaired and machine returns to operation;

Simulation runs until simulation time reaches mission time T_M. In the end of simulation failures that cause the machine to enter in a hazardous state are counted as the Number of failures at time T_M, $N(T_M)$. Each transition to a hazardous state counts as one dangerous control system failure; that is, $N(t)$ is increased by 1. In the example of figure 23 the events at time t_4, t_9 and t_12 are considered as dangerous and $N(T_M)$ equals 3.

Simulation has to be repeated for N times, where different event sequences occur. At the end of all simulations, $N(T_M)$ is averaged through the number of simulations N, resulting in an estimate of the expected number of failures,$\hat{E}(N(T_M))$. PFH is calculated by dividing $\hat{E}(N(T_M))$ by T_M, as in equation 2.29.

3.3 TOOLS

BlockSim is a software from Reliasoft that allows construction of RBD and evaluation of reliability measures for these diagrams. It is used as an evaluation tool. It offers support for non-repairable and repairable systems, and also provide simulation capabilities. A structure is simulated through discrete event simulation, where random times to failure for each block are generated following its failure distribution. After each failure, the overall behavior of the system (working or failure) is analyzed based on the state of each component and the structure.

BlockSim allows modeling of time to failure distributions, time to repair distributions for each block, different distributions, events that trigger repair and maintenance actions. It does not have resources for modeling events as tests, demands nor for duration of events, as tests duration, demands duration and time to failure detection. Therefore, some simplification hypothesis are used:

1. A failure due to common cause leads to the failure of the safety function, and cannot be detected;

2. Only dangerous failures are considered. Failures and repairs that do not impair the safety function are not accounted;

3. Failure modes are separated in detectable and undetectable. A detectable failure mode will always be detected. An undetectable will never be detected, independent of how many tests are performed;

4. Automatic tests are instantaneous;

5. A detected failure always leads the system instantaneously to safe state;

6. Repair begins instantaneously once in safe state;

7. An undetected failure does not lead to the failure of the safety function, in the case of redundant structures;

8. Two undetected failures are detected by a demand of the safety function, in the case of redundant structures;

9. Demand is continuous;

3.4 METHOD FOR CALCULATION OF PFH WITH RELIABILITY BLOCK DIAGRAMS AND SIMULATION

A calculation method is presented in this section. It is a sequence of steps for setting up simulation. Detailed explanation of each method step is given in the sequence.

Method: Method for PFH calculation with BlockSim

Data: Parameters of failure distribution of each component, DC of each component, mission time T_M

Result: PFH

1 Model the RBD;
2 Determine intrinsic parameters;
3 Determine failure parameters of each block (see sub-steps);
4 Determine number of simulations;
5 Set simulation end time to mission time;
6 Convert simulation results into PFH;

Figure 24 – Model for category B and category 1

3.4.1 Model the RBD

In principle, ISO 13849 allows application of any architecture, since they fulfill the requirements of the categories. The categories have the designated architectures, which are a guidance to design, but they are not mandatory. Any architecture which has the same failure behavior is allowed.

Nevertheless, in order to enable a better understanding, two fixed RBD are suggested for the calculation here presented. One RBD models categories B and 1, and the second suggested RBD models for categories 3 and 4. These RBD are used for PFH calculation both with exponential or Weibull distributed failures.

For categories B and 1, figure 24 shows how it is represented.

This model is very simple, comprising only one block, which may represent a single component or a whole channel. It is suitable for these categories because there is no redundancy, nor detection of failures. Once the channel fails, a demand of the safety function reveals the failure, and it must be repaired. The time to repair must be specified as well.

For categories 3 and 4, a 1oo2[3] RBD is used to represent a structure with single fault tolerance, detection of failures and failures due to common cause. This is represented in figure 22. Failure of each block is now described by a Weibull distribution.

The block diagram contains two channels to represent redundancy (fault tolerance), where each channel is composed by two failure modes, detected and undetected, and a series block to represent common cause failures of both channels, as represented in figure 22. This model is equivalent to the block diagram representation of a 1oo2 architecture, from IEC 61508-6 (International Electrotechnical Comission, 2010b).

Association to failure and repair parameters is discussed in the next sections.

[3] 1oo2 stands for 1 out of 2, which means that out of 2 channels, one must not fail in order to fulfill the function.

3.4.2 Determine intrinsic parameters

As discussed in section 3.1, there are other parameters than category, $MTTF_d$ and DC_{avg} that were used to generate the models used to calculate PFH in ISO 13849. As their order of magnitude is much lower than $MTTF_d$, their absolute value does not influence strongly in PFH calculation. However, PFH is a measure of repairable systems, and no consideration of repair (and repair rate) and test (and test frequency) leads to wrong results.

As there is no study in the scope of the ISO 13849 and no reference of what is acceptable for compliance with the standard, the same values used in ISO 13849 are used here. These values, while are not given by the standard, are mentioned by the STSARCES Report (DORRA; REINERT, 2000) and by the BGIA Report 2/2008e (HAUKE et al., 2009).

As safety-related controls are integrated to machinery, once a failure occurs, they must be repaired in order to the machine be able to be operated again. Therefore, a safety function must be modeled as a repairable system. In a repairable model, it is necessary to specify the repair time as well. Repair times are assumed to be random, following a exponential distribution, with mean time of 8 hours.

Common cause failures are assumed to be represented by the Beta-factor model (refer to section 2.1.16). For the machinery sector, it is estimated that a factor of 2% is realistic, which is assumed in the case of compliance with the process described in Annex F of ISO 13849. It is not allowed to design a redundant safety function that do not comply to this process.

Mission time, T_M, is assumed to be 20 years. For the case of Weibull distribution, other values of mission time are considered, in order to evaluate possible effects.

As discussed in section 3.3, BlockSim version 6.5 does not have resources for modeling periodic demands or tests. The effect of a failure of a block is evaluated at the time point it occurs, meaning that a detected failure mode is instantaneously detected, what corresponds to continuous testing, with no duration. A failure of the overall safety function is detected instantaneously, what corresponds to the case of continuous demand.

A summary of intrinsic parameters in given in table 5.

Table 5 – Summary of intrinsic parameters

Parameter	Value
Demand rate	Higher than 1 demand per year
Repair rate μ	1 repair each 8 hour
Test frequency	-
Common cause failure factor β_{CCF}	2%
Mission time T_M	20 years

3.4.3 Determine failure parameters of each block

Failure parameters are dependent of category, the number of blocks in each model and the failure distribution that is assigned for each block. Therefore, failure parameters have to be determined individually for each case.

In the next sections, failure parameters are determined regarding to each category and failure distribution. Sub-steps for step 3 are listed.

3.4.4 Determine number of simulations

A simulation run is a realization of random failure and repair times. The safety function (modeled by the RBD) keeps failing and being repaired, until the selected time for the end of the simulation. Simulation end time is equivalent to the mission time of the control system. Repeating this process many times generates data enough to derive statistics of the safety function.

From the simulation, the expected number of failures is estimated. This estimate is used as the expected number of failures in equation 2.29.

$$E(N(T_M)) = \hat{E}(N(T_M)) \tag{3.1}$$

Number of simulations has to be set according to the desired precision. This is accomplished by the equation:

$$N_{sim} = \frac{1}{\epsilon_{PFH} \cdot T_M} \tag{3.2}$$

Where N_{sim} is the number of simulations, ϵ_{PFH} is the desired precision

for PFH result and T_M is the mission time.

3.4.5 Convert simulation results into PFH

The output of interest in the simulation is the expected number of failures. From this result, it is possible to calculate PFH via equation 2.29. As mission time for the safety function is considered 20 years in the scope of the ISO 13849, the expected number of failures must be divided by this value in hours, which is 175200 hours.

Besides expected number of failures, BlockSim gives standard deviation for the calculated expected number of failures. From IEC 61508-6, a 90% confidence interval for estimated mean is given by:

$$Conf_{E(N(t))} = 1.64 \cdot \frac{\sigma_{E(N(t))}}{\sqrt{N}} \tag{3.3}$$

Where $Conf_{E(N(t))}$ means the confidence interval, $\sigma_{E(N(t))}$ is the standard deviation of the expected number of failures, calculated by BlockSim, and N is the number of simulations.

Equation 3.3 can be adapted to an equation for the 90% confidence interval for PFH, as given:

$$Conf_{PFH} = 1.64 \cdot \frac{\frac{\sigma_{E(N(t))}}{175200}}{\sqrt{N}} \tag{3.4}$$

3.5 COMPARISON BETWEEN ISO 13849 AND PROPOSED METHOD

In order to confirm that the proposed method deliver correct results, i.e. the same results from ISO 13849 for the same inputs, PFH is calculated for categories B, 1, 3 and 4, for the whole range of MTTF_d and DC_{avg} values.

3.5.1 Catergory B or 1

PFH is calculated for category B, for the range of MTTF_d values from 3 to 27 years, and for category 1, MTTF_d ranging from 30 to 100 years. These are the same values presented in table K.1 from ISO 13849. Diagram block from figure 24 is used, meaning that only $\lambda_d = {}^1/_{MTTF_d}$

has to be specified.

A PFH result is considered valid if it fall under the same PL as its respective reference PFH value from the standard. For a discussion about validation of results, see appendix E.

Calculation results are displayed in figure 26. This figure is also displayed in tabular form, in table 12, in appendix E.

As it can be seen in figure 26, all the cases for category B and 1 result in the same PL for the calculated and reference PFH. This method is therefore considered satisfactory.

3.5.2 Catergory 3 or 4

For this method, the RBD from figure 22 is used. In this RBD, there are 5 blocks whose failure parameters have to be defined.

As input parameters, category, overall MTTF_d and DC_{avg} are used. Category is already considered in the RBD. From the MTTF_d and the DC_{avg} the five failure distribution parameters are derived. For all 5 blocks, an exponential failure rate is assumed. Therefore, an MTTF_d for each block is needed.

Although the standard is written in terms of MTTF_d, usage of failure rate provides simpler algebraic manipulation. Therefore, for the exponential failure distribution, the relation

$$\lambda_d = \frac{1}{MTTF_d} \tag{3.5}$$

is used allow usage of failure rates.

Figure 25 represents this approach of failure parameters derivation.

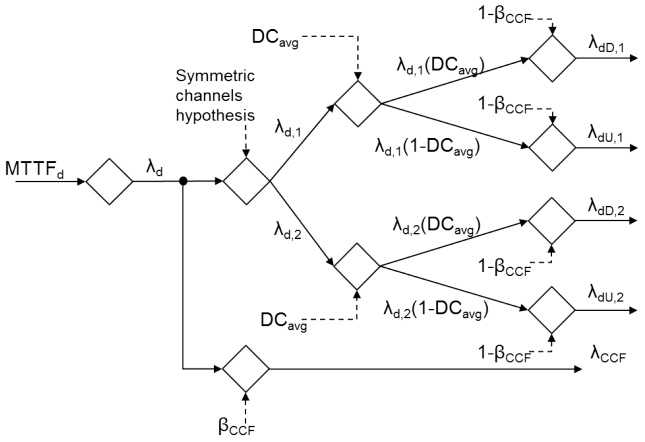

Figure 25 – Representation of the determination of the failure rates for each block

Failure rate λ_d represents the overall failure rate, for both channels. The proportion of failures due to common cause is given by β_{CCF}, and is deducted from the overall failure rate. This results in

$$\lambda_{CCF} = \lambda_d \cdot \beta_{CCF} \tag{3.6}$$

and

$$\lambda_{independent} = \lambda_d \cdot (1 - \beta_{CCF}) \tag{3.7}$$

Failure rate λ_{CCF} from equation 3.6 is the failure rate of block E from figure 22.

From the independent proportion of failure rate, it is considered that both channels have the same failure rate, and that it is equal to the independent failure rate. This assumption is not correct, because components in parallel with exponential distribution do not result in a system with exponential distribution, making equation 3.5 invalid, and because an equivalent MTTF would be higher than MTTF of both channels, given by

$$MTTF_{system} = MTTF_{Ch1} + MTTF_{Ch2} - \frac{1}{\frac{1}{MTTF_{Ch1}} + \frac{1}{MTTF_{Ch2}}} \tag{3.8}$$

according to (BILLINTON; ALLAN, 1992). It can be shown that, when $\text{MTTF}_{Ch1} = \text{MTTF}_{Ch2}$, MTTF_{system} is 1.5 times higher than both

MTTF.

However, ISO 13849 has an conservative approach, and it introduces an factor of 2/3 in the MTTF_d symmetrization equation, as reproduced again:

$$MTTF_d = \frac{2}{3}\left[MTTF_{d,C1} + MTTF_{d,C2} - \frac{1}{\frac{1}{MTTF_{d,C1}} + \frac{1}{MTTF_{d,C2}}}\right] \tag{3.9}$$

It can be shown in equation 3.9 that if $\text{MTTF}_{Ch1} = \text{MTTF}_{Ch2}$, then $\text{MTTF}_{d,Ch1} = \text{MTTF}_{d,Ch2} = \text{MTTF}_d$. Because of this conclusion, failure rates of each channel are assumed to be equal to the overall independent failure rate.

As all of the dangerous failure modes can be divided into detected and undetected, the following equation applies

$$\lambda_d = \lambda_{d,D} + \lambda_{d,U} \tag{3.10}$$

Substituting equation 3.10 in 2.33 leads to

$$\lambda_{d,D} = \lambda_d \cdot DC_{avg} \tag{3.11}$$

and

$$\lambda_{d,U} = \lambda_d \cdot (1 - DC_{avg}) \tag{3.12}$$

Manipulating equations 3.7, 3.11 and 3.12 leads to

$$\lambda_{dD} = \lambda_d \cdot DC_{avg} \cdot (1 - \beta_{CCF}) \tag{3.13}$$

for the blocks A and C of figure 22, and

$$\lambda_{dU} = \lambda_d \cdot (1 - DC_{avg}) \cdot (1 - \beta_{CCF}) \tag{3.14}$$

for the blocks B and D.

Resulting sub-steps for step 3 of proposed method (section 3.4 are:

Sub-method: Sub steps for step 3 of calculation method
3.1 Calculate $\lambda_d = \frac{1}{MTTF_d}$;
3.2 Calculate $\lambda_{CCF} = \lambda_d \cdot \beta_{CCF}$;
3.3 Calculate $\lambda_{dD} = \lambda_d \cdot DC_{avg} \cdot (1 - \beta_{CCF})$;
3.4 Calculate $\lambda_{dU} = \lambda_d \cdot (1 - DC_{avg}) \cdot (1 - \beta_{CCF})$;

Results for category 3 with DC_{avg} of 60% and 90%, and for category 4 were calculated, and are displayed in figure 26. The same results are presented in a table in appendix E.

For category 3 with DC_{avg} of 60% deviation was high enough, specially for low $MTTF_d$ values, to generate cases with different PL. This happens with the cases where the reference PFH was close to the transition value of one PL to another, namely $MTTF_d$ of 11 and 24 years. As the calculated PL is lower than the reference, the calculated value is conservative and therefore, acceptable.

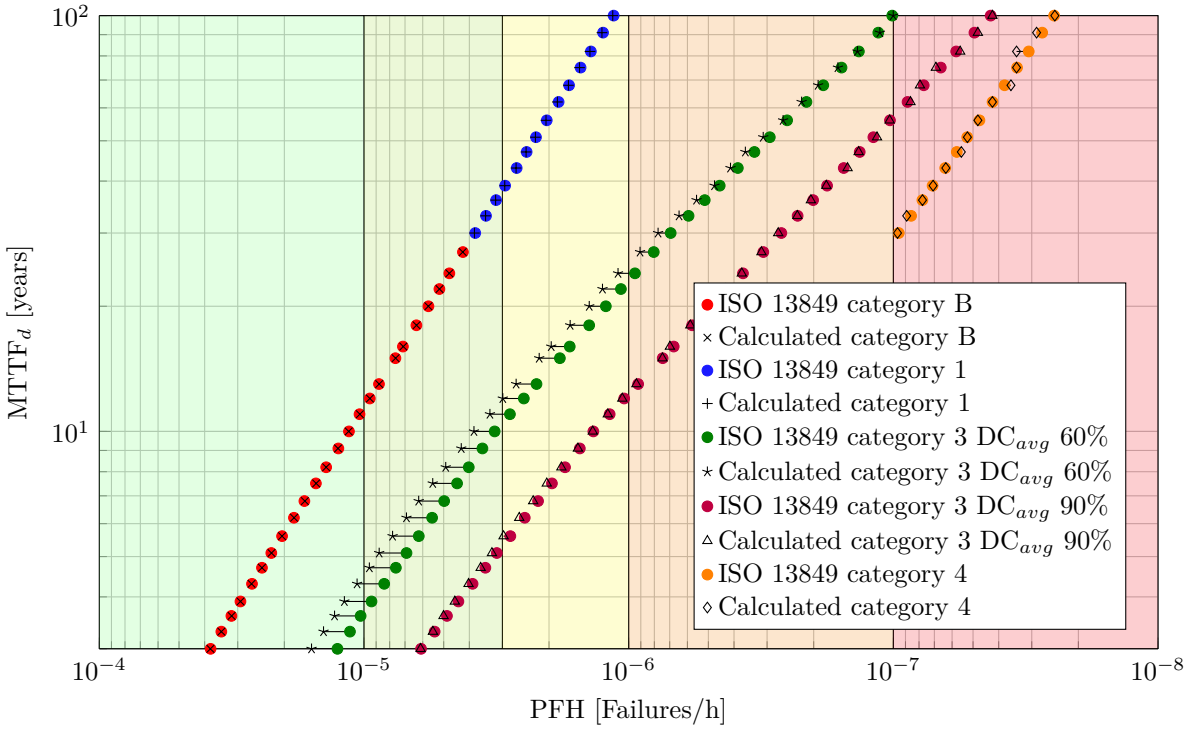

Figure 26 – Comparison of PFH values of ISO 13849 and calculated through BlockSim for all calculated categories. Intervals that represent different Performance Levels are shaded in different colors.

3.6 USE OF WEIBULL DISTRIBUTION

Impact of Weibull distribution is just on failure parameters of each block (Figs. 22 and 24). Therefore, just step 3 has to be adapted. Failure parameters are dependent of the system and analysis has to be performed for each case.

Although there is no reference to compare whether calculated values are correct for category B and 1, it provides insight of influence of Weibull distribution in PFH. For an application example of categories 3 and 4, refer to chapter 4.

3.6.1 Catergory B or 1 with Weibull distribution

Instead of entering failure rate or MTTF_d for the block, parameters η and β_W of the Weibull distribution have to be specified. These parameters can be specified by a failure field analysis (Weibull analysis), as proposed by Orth and Raksch (ORTH; RAKSCH, 2014).

Parameters of the Weibull distribution must be known for this method. Although accuracy of results is strongly dependent of accuracy of input data, origin of η and β_W parameter do not have influence on the method here presented.

Sub-method: Sub steps for step 3 of calculation method considering category B or 1 with Weibull distribution
3.1 Assign η and β_W to the block;

In the present method, the mission time becomes an explicit parameter. Assumption of Weibull distribution models wear-out effects, removing the limitation of the useful life. As the failure rate changes with time, PFH varies as well, and it becomes important to specify to which mission time the safety function is designed.

For this method, only theoretical values were considered, in order to evaluate the effect of Weibull distribution. Four cases were simulated, for different mission times. They are represented in table 6.

The characteristic lifetime η is based in the typical MTTF_d for hydraulic valves suggested by ISO 13849, which is 150 years. This value is however capped to 100 years, as this is the maximal allowed for each channel of a safety function, in the current version of the standard.

To find an equivalent Weibull distribution to MTTF_d of 100

Table 6 – Assignment of Performance Level according to PFH

Characteristic lifetime η	100 years
Shape parameter β_W	1; 1,3; 1,5 and 2
Mission time (Simulation stop time)	From 1 to 30 years
Number of simulations	50000

years, the point of 63% of failures was chosen. In the exponential distribution, this point is represented by the MTTF_d, considering only dangerous failures. That means, in 100 years, there would be 63% of failed items. The point of 63% of failures in the Weibull distribution is given by η. This can be demonstrated substituting η as time in equation 2.16 of the cumulative probability distribution, resulting in

$$F(\eta) = 1 - e^{-\left(\frac{\eta}{\eta}\right)^{\beta}} = 1 - e^{-(1)^{\beta}} = 1 - e^{-1} = 0,6321... \tag{3.15}$$

Therefore, η was chosen as 100 years.

Values for the shape parameter were chosen based in common values for hydraulic valves, provided by preliminary studies from Bosch Rexroth, as presented by Orth and Raksch (ORTH; RAKSCH, 2014).

Resulting failure rates are represented in figure 27. PFH results are given in figure 29.

Resulting PFH values for each of the four cases are displayed in figure 29. For each different mission time, it is calculated the average PFH from 0 to the mission time (e.g. for 5 years, the average from 0 to 5 years; for 10 years, the average from 0 to 10 years of operation).

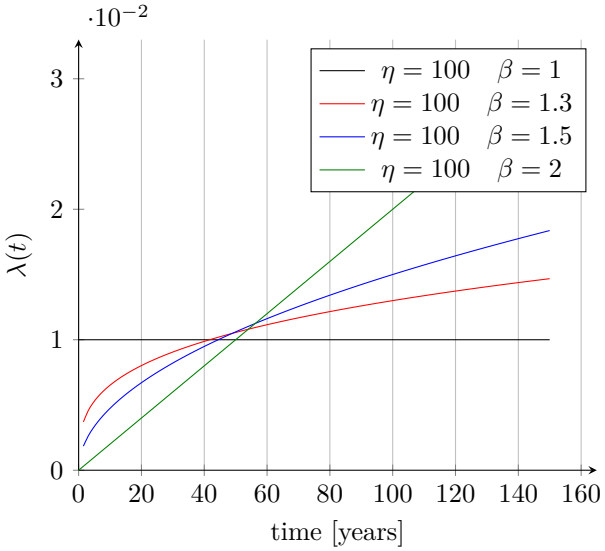

Figure 27 – Failure rate of the four analyzed cases

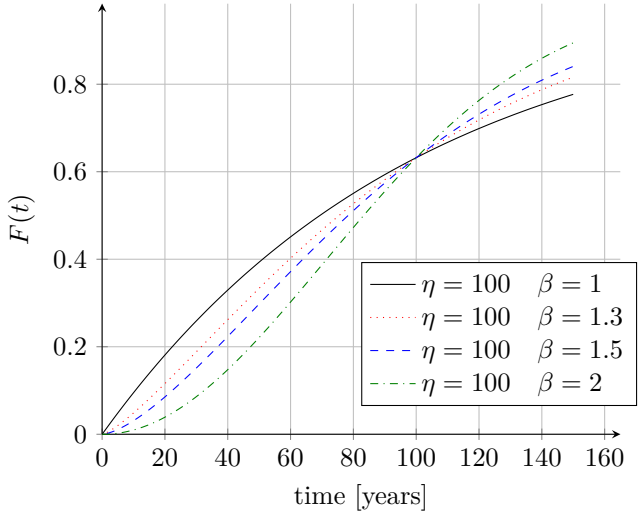

Figure 28 – Failure distribution of the four analyzed cases

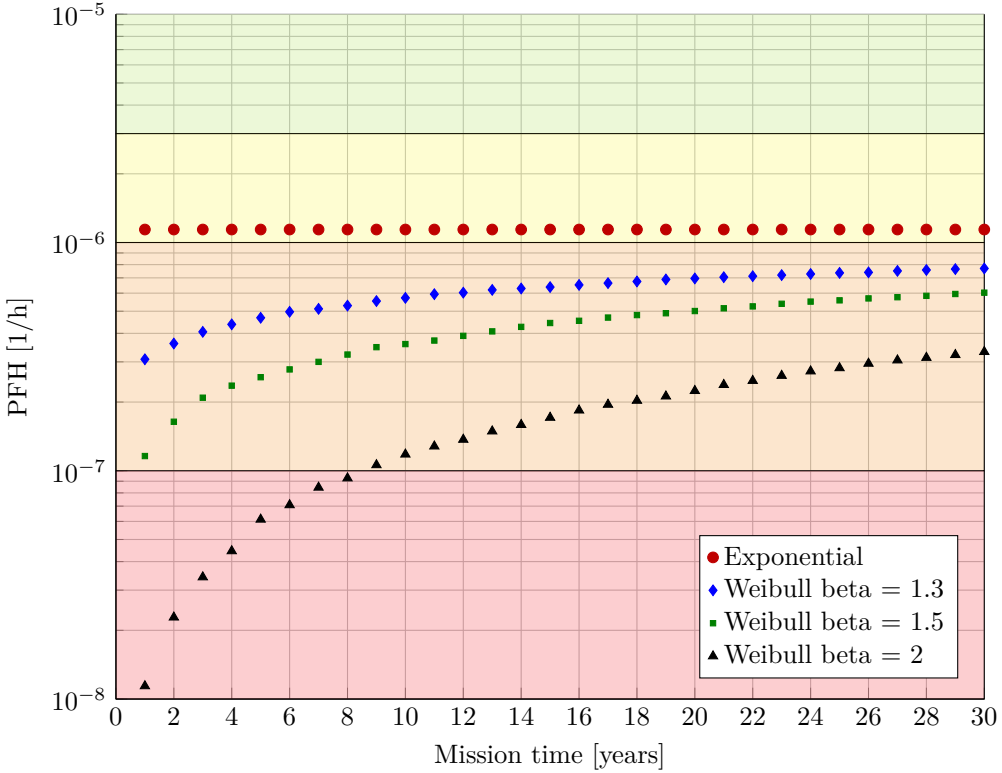

Figure 29 – PFH calculated for different mission times

It can be seen that for lower mission times and higher shape parameters (β_W), the PFH increases. This effect is due to low failure rates in the beginning of life of components. As time increases, failure rates of components increases, as represented by figure 27, and PFH increases as well.

3.6.2 Catergory 3 or 4 with Weibull distribution

This method is intended to calculate PFH for a redundant architecture with Weibull distribution. It is suitable for safety functions implemented with redundant component, as a control block with 2 hydraulic valves.

Additional hypotheses are considered in order to obtain failure parameters for each block. They are:

1. Detected and undetected failure modes have the same distribution type as the respective component;
2. The distribution of a component can be written as a combination of the distribution of its failure modes;
3. Shape parameter β_W of failure modes are the same as the shape parameter β_W of a component;

Each block is described by two parameters, η and β_W. As there are 5 blocks in the RBD, there are 10 block parameters. In order to avoid confusion, each parameter is referred with a subscript of its respective block. Considering it, the problem becomes determination of η_A, $\beta_{W,A}$, η_B, $\beta_{W,B}$, η_C, $\beta_{W,C}$, η_D, $\beta_{W,D}$, η_E and $\beta_{W,E}$.

These parameters are given by the equations 3.16 to 3.25. For these equations, it is assumed that channels are not symmetric, i.e. each component has a different distribution, and that diagnostic coverage is different also for each component. Therefore, DC must be specified for each component.

Reason for choosing to keep equations based on failure and detection parameters for each component is that these parameters are indeed calculated during design. Deduction of equations from 3.16 to 3.25 can be found in appendix D.

A specific method for PFH calculation with Weibull distribution is given.

$$\eta_A = \eta_{dD,Ch1} = \frac{\eta_{Ch1}}{\sqrt[\beta_{W,Ch1}]{DC_{Ch1}(1-\beta_{CCF})}} \tag{3.16}$$

Sub-method: Sub steps for step 3 of calculation method considering category 3 or 4 with Weibull distribution
3.1 Calculate η_A and $\beta_{W,A}$ (Eqs. 3.16 and 3.17);
3.2 Calculate η_B and $\beta_{W,B}$ (Eqs. 3.18 and 3.19);
3.3 Calculate η_C and $\beta_{W,C}$ (Eqs. 3.20 and 3.21);
3.4 Calculate η_D and $\beta_{W,D}$ (Eqs. 3.22 and 3.23);
3.5 Calculate η_E and $\beta_{W,E}$ (Eqs. 3.24 and 3.25);

$$\beta_A = \beta_{W,dD,Ch1} = \beta_{W,Ch1} \tag{3.17}$$

$$\eta_B = \eta_{dU,Ch1} = \frac{\eta_{Ch1}}{\sqrt[\beta_{W,Ch1}]{(1 - DC_{Ch1})(1 - \beta_{CCF})}} \tag{3.18}$$

$$\beta_B = \beta_{W,dU,Ch1} = \beta_{W,Ch1} \tag{3.19}$$

$$\eta_C = \eta_{dD,Ch2} = \frac{\eta_{Ch2}}{\sqrt[\beta_{W,Ch2}]{DC_{Ch2}(1 - \beta_{CCF})}} \tag{3.20}$$

$$\beta_C = \beta_{W,dD,Ch2} = \beta_{W,Ch2} \tag{3.21}$$

$$\eta_D = \eta_{dU,Ch2} = \frac{\eta_{Ch2}}{\sqrt[\beta_{W,Ch2}]{(1 - DC_{Ch2})(1 - \beta_{CCF})}} \tag{3.22}$$

$$\beta_D = \beta_{W,dU,Ch2} = \beta_{W,Ch2} \tag{3.23}$$

$$\eta_E = \eta_{CCF} = \frac{\eta_{AUX}}{\sqrt[\beta_{W,AUX}]{\beta_{CCF}}} \tag{3.24}$$

$$\beta_E = \beta_{W,CCF} = \beta_{W,AUX} \tag{3.25}$$

s To the present date, there is no known work on the consideration of Weibull distributed failures for PFH calculation of a redundant architecture for safety functions, neither under the scope of ISO 13849 nor IEC 61508. Additionally to this, it is impracticable to demonstrate the results through experiments. Due to these two factors, the presented method remains without verification.

In the next chapter, the presented method is applied to calculate

PFH for a hydraulic machine. Results are compared with the method provided by the ISO 13849 standard.

4 CASE STUDY OF A HYDRAULIC CONTROL SYSTEM

In this section, it is investigated the PFH of a hydraulic control system. At a first moment, the control system is analyzed by method of ISO 13849. After that, analysis is made with the method of section 3.6.2, when Weibull distribution is used for modeling components' failures. Only the quantitative aspects are considered in this work. The qualitative aspects are as important as the quantitative, but they are out of the scope.

This chapter is organized in the following manner: First, a description of the system. Second, a description of the proposed safety function. In the sequence, PFH is calculated following the ISO 13849 method. After, PFH is calculated following the proposed method. At the end, results are compared and analyzed.

As in figure 21, mission time T_M is made an explicit parameter.

4.1 SYSTEM DESCRIPTION

The system to be studied is a test stand from the Laboratory of Hydraulic and Pneumatic Systems(Laboratório de Sistemas Hidráulicos e Pneumáticos - LASHIP) from the Federal University of Santa Catarina (Universidade Federal de Santa Catarina - UFSC). It is an existing installation, that can be seen in figure 30. It is described by Gonzalez (GONZALEZ, 2012).

A new hypothetical application as a test stand would require it to follow the EHSR from Machinery Directive or NR12, what includes designing the control system according to ISO 13849.

Purpose of this new test stand is to perform endurance tests of mechanical components with controlled force and torque. The component to be tested is cyclically loaded by a hydraulic cylinder. Duration of each cycle is 30 seconds. The test stand is intended to operate continuously until the test termination criteria is met, or a stop by safety reasons is necessary. The hydraulic circuit responsible for driving the cylinders is shown in figure 31.

In order to reduce risks of harms due to moving parts, a stop must be triggered when someone is in the surroundings of the machine. This reaction configures a safety function. Not only one safety function is required in order to reduce risks associated to the hydraulic test

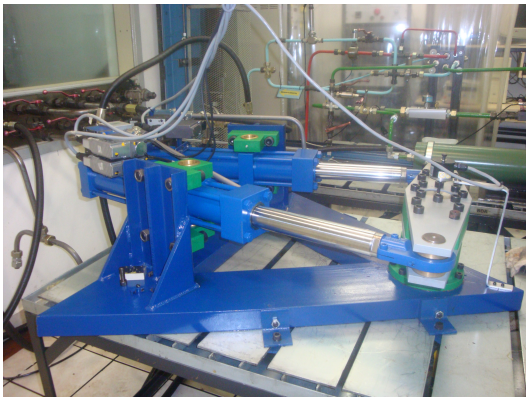

Figure 30 – Picture of the LASHIP test stand

stand. However, only the function **Safety-related stop initiated by a safeguard** is analyzed in this work.

Previous studies concluded that this application requires PL d (refer to table 2 and figure 5). In the next section, the safety function is designed to meet the integrity, i.e. quantitative requirements of the ISO 13849. That is, only PFH to meet the required PL is calculated; there is no concern in this work to software and systematic failures, nor to the effectiveness of the function (response time, etc.).

4.2 DESIGN OF SAFETY FUNCTION

A safety-related stop is required when a person is in the surroundings of the test stand. A pressure mat and a safety relay are used to detect presence of persons in the hazardous area and trigger a stop signal to the hydraulic circuit.

The function is implemented by modules that already implement a partial safety function. The overview of the safety function can be seen in figure 32. The sensor sub-function is implemented by a safety mat, that detects presence in the surroundings. The logic sub-function is implemented by a safety relay, which monitors both channels of the safety mat, and implement other safety functions, like manual reset, but that are not important for this analysis. For both sensor and logic sub-functions, components are already constructed to meet requirements of category 3 and 4 and PL d and e.

In order to achieve PL d for the safety function, it is necessary to

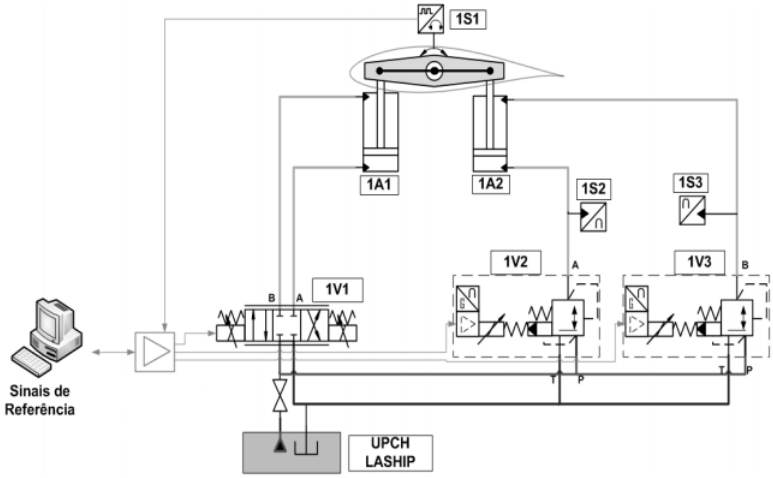

Figure 31 – Schematics of the original hydraulic circuit. Reproduced from Gonzalez (GONZALEZ, 2012)

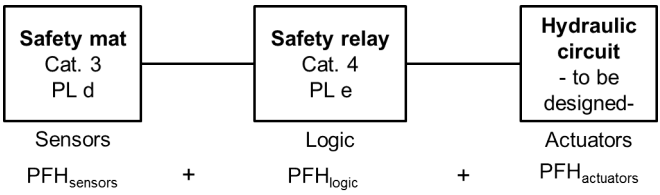

Figure 32 – Architecture of the proposed safety function

achieve PL d for the hydraulic circuit as well. For that, it is necessary to design the actuator subsystem with category 2 or 3, as presented in the bar chart of figure 20. Category 3 is preferred, which implies in realization of the safety function with tolerance against single failure, that is, redundancy in the realization of the safety function.

In the case of a safety-related stop, redundancy means stopping both cylinders by two different (and independent means). As the cylinders are coupled, it is necessary block hydraulic fluid flow to one of them.

A stop can be accomplished by valve 1V1. Due to constructive measures[1], the valve is suitable for a safety reaction (stop reaction). As valves 1V2 and 1V3 are pressure reducing valves, they are not capable of block hydraulic fluid flow, and cannot stop the system's movement.

Therefore, an additional mean to stop the cylinders is needed.

In order to provide a second function channel, an additional valve is proposed. The resulting circuit is shown in figure 33. Diagnostics of the circuit is provided by spool-position of valve 1V1, encoder 1S1, pressure sensors 1S2 and 1S3, and solved by the controlling computer.

A proposal for the hydraulic circuit is shown in figure 33. The resulting RBD of the actuator subsystem is shown in figure 34.

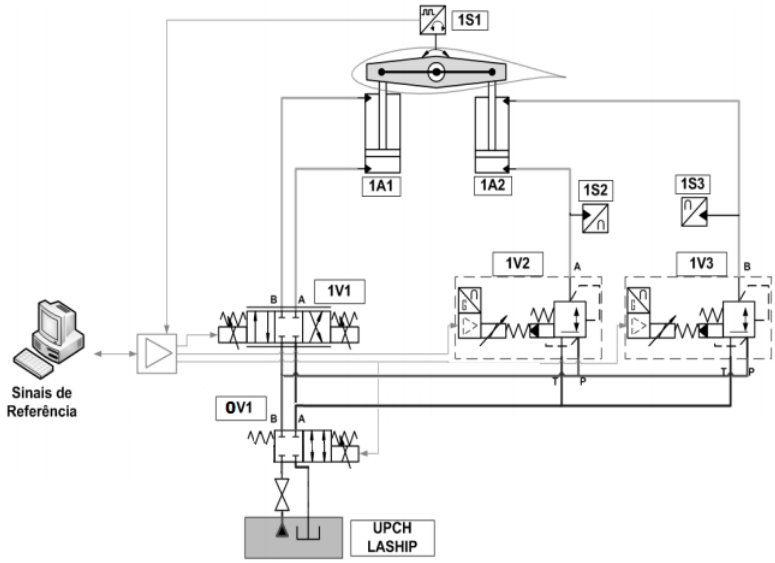

Figure 33 – Schematics of the proposed hydraulic circuit

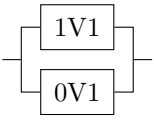

Figure 34 – Redundancy by two hydraulic valves performing a safety-related stop

[1]This valve has sufficient overlapping and is spring-centered, blocking flow in the centered position when power is removed from its solenoids.

4.3 PFH CALCULATION ACCORDING TO ISO 13849

In order to estimate PFH according to ISO 13849, it is necessary to estimate 3 parameters: category, DC_{avg} and $MTTF_d$. The first two are already determined. Therefore, it is necessary to estimate overall $MTTF_d$ of the hydraulic circuit.

4.3.1 $MTTF_d$

$MTTF_d$ of hydraulic valve should be determined by the component manufacturer. It should be determined via lifetime testing. However, the standard states that given that hydraulic valves are manufactured according to safety principles and with appropriate materials and quality control processes, a value of 150 years can be claimed. $MTTF_d$: each valve fulfill the safety principles, and therefore each can claim 150 years for $MTTF_d$. However, the maximal $MTTF_d$ for each channel is 100 years.

As each channel consists of one unique valve each,

Using equation 2.31, 100 years for $MTTF_d$ for both channels is obtained.

4.3.2 DC_{avg}

In the scope of ISO 13849, Diagnostic Coverage is estimated for each item according to failure detection measures implemented. These measures are listed in annex E of the standard. Valve 1V1 has an integrated sensor for the position of the internal spool. Monitoring of control valves is regarded as achieving 99% of detected failures.

Valve 0V1 has no spool position sensor. Failures of the valve are indirectly detected by other means, as listed:

- Daily test of 0V1: Before automatic operation, 1V1 is left open and a movement sequence is given to the control valve. Power is removed from 0V1. If the cylinders stop, what can be monitored by encoder 1S1, the valve is working properly. If the cylinders continue to move, the valve has failed to danger and must be changed.

- Demand of the safety function: When both 1V1 and 0V1 close, flow and cylinders stop and pressures in 1S2 and 1S3 are kept

constant. In the case of malfunction, pressures in both sensors continue to vary according to the setpoints in the application software.

Monitoring of failure in valve 0V1 corresponds to indirect measures, and achieve 60% of detected failures, according to annex E of ISO 13849.

With DC of each component, DC_{avg} is determined by equation 2.34

$$DC_{avg} = \frac{\frac{0.99}{100} + \frac{0.60}{100}}{\frac{1}{100} + \frac{1}{100}} = 79.5\% \tag{4.1}$$

According to the classification (see table 4), the calculated value corresponds to low DC_{avg}.

4.3.3 Common cause failures

In order to guarantee the common cause factor β_{CCF} of 2%, it is necessary to use the process of Annex F of ISO 13849.

4.3.4 PFH estimation

From table K.1, with category 3, DC_{avg} low and $MTTF_d$ of 100 years, the value of $1.01 \cdot 10^{-7}[1/h]$. This PFH value assumes mission time T_M of 20 years. It is reproduced in appendix E of this work, table 13.

4.4 PFH CALCULATION ACCORDING TO PROPOSED METHOD

A preliminary study from Bosch Rexroth was conducted considering analysis of field failure records for the corresponding valves. Failure parameters were estimated by Weibull analysis, considering dangerous failure modes only. Diagnostic coverage was estimated based on the proportion of failures modes that are detectable. Due to confidentiality, real values cannot be used. Nevertheless, values shown in table 7 are considered to be realistic for the application.

Three cases are considered: Case 1 refers to two valves, which are regarded to be slightly less prone to failures as valves from Case 2. Case 3 refers to the of not having position monitoring on shut off valve.

Table 7 – Summary of failure distribution parameters as input for case studies of a hydraulic actuator subsystem

	Directional valve 1V1			Shut off valve 0V1			CCF
Case	η_{Ch1}	$\beta_{W,Ch1}$	DC_{Ch1}	η_{Ch2}	$\beta_{W,Ch2}$	DC_{Ch2}	β_{CCF}
1	30 y	2	90 %	45 y	2.8	99 %	2 %
2	24 y	2	90 %	40 y	2.4	90 %	2 %
3	24 y	2	90 %	40 y	2.4	60 %	2 %

Table 8 – Simulation parameters

Parameter	Value
Mean repair time (MRT)	8 hours
Demand rate	Continuous
Test rate	Continuous

4.4.1 Model the RBD

In this case, the RBD proposed in figure 22 is used. It can be seen modeled in BlockSim version 9 in figure 35.

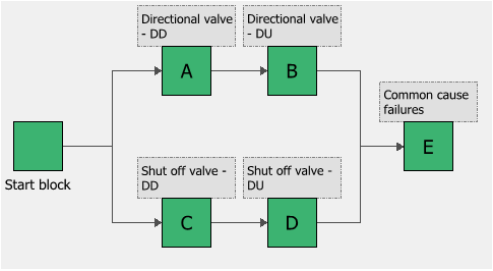

Figure 35 – 5-block RBD for a redundant actuator subsystem for safety

4.4.2 Determine intrinsic parameters

The intrinsic parameters are kept as in ISO 13849. They are summarized in table 9.

Table 9 – Parameters for the block diagram

	Case 1	Case 2	Case 3
η_A	31.9438 y	24.3658 y	24.3658 y
β_A	2	2	2
η_B	95.8315 y	242.437 y	242.437 y
β_B	2	2	2
η_C	45.4888 y	42.1484 y	49.9060 y
β_C	2.8	2.4	2.4
η_D	234.764 y	105.289 y	59.0914 y
β_D	2.8	2.4	2.4
η_E	141.123 y	144.875 y	144.875 y
β_E	3.62	3.17	3.17

4.4.3 Determine failure parameters of each block

Failure parameters for each block are calculated with values given in table 7, with equations from 3.16 to 3.25. Results in table 9.

4.4.4 Determine number of simulations

It is expected to achieve PFH results up to PL e limit, which is $10^{-8}[^1/_h]$ in 20 years[2]. The desired increment ϵ_{PFH} is $10^{-10}[^1/_h]$. From equation 3.2

$$N_{sim} = \frac{1}{10^{-10} \cdot 175200} \approx 57078 \tag{4.2}$$

Simulation number was chosen 60000, which leads to ϵ_{PFH} of $1.14 \cdot 10^{-10}[^1/_h]$, considered acceptable.

4.4.5 Set simulation end time to mission time

Different mission times were used, in order to evaluate effects in PFH. PFH is calculated as an average for each lifetime span, ranging from 1 to 20 years of operation. Mission times are set as the time to stop the simulation.

[2] 175200 hours

Table 10 – Calculated PFH with 90% confidence interval for actuator subsystem considering mission time of 20 years

	Calculated PFH	90% confidence interval	Lower PFH	Upper PFH	PL
Case 1	1.85E-8	2.4E-9	1.61E-8	2.09E-8	e
Case 2	3.80E-8	3.4E-9	3.46E-8	4.14E-8	e
Case 3	9.84E-8	5.4E-9	9.30E-8	1.039E-7	d

4.4.6 Convert simulation results into PFH

BlockSim calculates $\hat{E}(N(t))$ and $\sigma_{E(N(t))}$. Therefrom is possible to estimate PFH and the 90% confidence interval for PFH. Results for PFH and confidence interval for mission time of 20 years is given in table 10. For PFH estimate for all mission times, see figure 36.

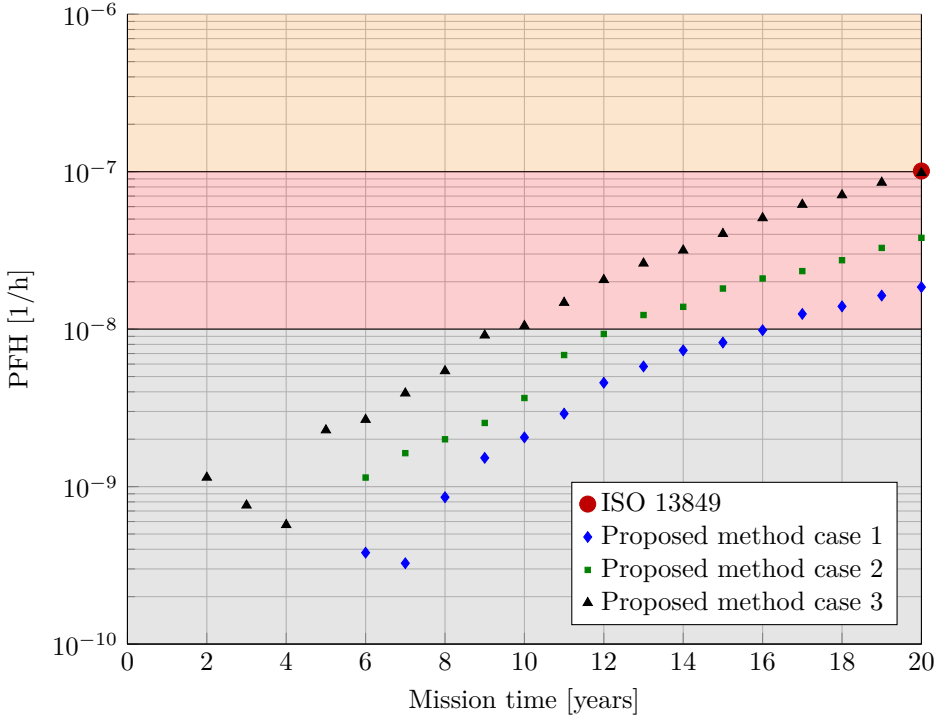

Figure 36 – Calculation of PFH for different components configurations and mission times. The orange area represents PL d, the red area represents PL e and the gray area has no correspondence in ISO 13849. For PFH estimation according ISO 13849, PFH is estimated just for mission time of 20 years.

4.5 ANALYSIS OF B_{10}

For the ISO 13849 procedure, PFH calculation is valid only within the B_{10} of each component. Result is the valve has to be changed after reaching B_{10} switching cycles. Bosch Rexroth's hydraulic valves are normally designed to achieve B_{10} of 10 million switching cycles (BOSCH REXROTH AG, 2012). After reaching this number of cycles, valve should be changed.

Recalling the system description in section 4.1, the expected duration of a cycle is 30s. Two cases are analyzed: 200 days or full year of continuous operation.

4.5.1 Case 200 days of operation per year

B_{10} is measured in cycles. To convert this value into years, it is necessary to estimate a mean operation frequency. ISO 13849-1 Annex C4 gives equations for estimating this frequency (International Organisation for Standardization, 2006).

$h_{op} = 24\ h$
$d_{op} = 200\ days$
$t_{cycle} = 30\ s$

$$n_{op} = \frac{d_{op} \cdot h_{op} \cdot 3600}{t_{cycle}} = \frac{200 \cdot 24 \cdot 3600}{30} = 576000[^{cycles}/_{year}] \quad (4.3)$$

$$\frac{B_{10}}{n_{op}} = \frac{10000000[cycles]}{576000[^{cycles}/_{year}]} = 17.36 years \quad (4.4)$$

According to ISO 13849, valves must be replaced after approx. 17 years. However, for cases 1 and 2, it is possible to maintain even PL e in a time of 20 years, without being necessary to replace the valves.

4.5.2 Case full year operation

In this case, time to replace the valves becomes lower.

$h_{op} = 24\ h$
$d_{op} = 365\ days$
$t_{cycle} = 30\ s$

$$n_{op} = \frac{d_{op} \cdot h_{op} \cdot 3600}{t_{cycle}} = \frac{365 \cdot 24 \cdot 3600}{30} = 1051200[^{cycles}/_{year}] \quad (4.5)$$

$$\frac{B_{10}}{n_{op}} = \frac{10000000[cycles]}{1051200[^{cycles}/_{year}]} = 9.51 years \tag{4.6}$$

While for case 1 and case 2 the calculated PFH lie around middle of interval for PL e, in case 3 the calculated PFH lies to near to the endpoint of interval. In fact, the upper PFH value is already outside the PL e interval. A conservative approach is to consider this system as reaching only PL d. A summary of achieved PL is given in Table 11.

While for case 1 and case 2 the calculated PFH lie around middle of interval for PL e, in case 3 the calculated PFH lies to near to the endpoint of interval. In fact, the upper PFH value is already outside the PL e interval. A conservative approach is to consider this system as reaching only PL d.

4.6 CALCULATION OF PFH FOR THE COMPLETE SAFETY FUNCTION

With PFH value of the actuator subsystem, it is possible to determine PFH and PL for the whole safety function. Values for the pressure mat with controller and for the safety relay are given by the component manufacturer.

$$PFH = PFH_{Sensors} + PFH_{Logic} + PFH_{Actuators} \tag{4.7}$$

Table 11 – Calculated PFH for the complete safety function

	ISO 13849	Case 1	Case 2	Case 3
Calculated PFH	1.09E-7	2.66E-8	4.61E-8	1.06E-7
Achieved PL	d	e	e	d

5 APPLICATION OF PROPOSED METHOD IN AN ENGINEERING PROJECT

The objective of this chapter is to analyze whether is feasible the usage of the developed techniques in the industry by machine builders and designers.

Safety functions are part of a bigger framework for risk reduction. It is based on the European Machinery Directive 2006/42/EC, which regulates the market of machinery in Europe, together with technical standards for risk assessment and risk reduction. Machines shall not pose hazards to people, and this is regulated by Essential Health and Safety Requirements, EHSR, stated in the Machinery Directive (EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION, 2006).

In this context, there is an effort in Bosch Rexroth to further develop Motion Simulation Systems to achieve higher levels of safety and improve documentation for the Machinery Directive. Therefor it is desired to provided integrated safety functions. In that way, safety functions are a ready-to-use product feature, reducing engineering effort from the system integrator and increasing the economic value added. Designing the system to some pre-programmed safety reactions, which are compliant[1] up to a certain Performance Level (PL) or Safety Intergrity Level (SIL) facilitates the design for the system integrator.

The system provided by Bosch Rexroth is a 6 degrees-of-freedom (DOF) motion platform, used for simulation of motion cues[2] for flight and driving simulation. Such platforms can be constructed in different sizes, with hydraulic or electric actuators, depending on the desired payload. An example of a motion platform can be seen in figure 37. Motion cues are generated based on position, velocity and acceleration set poitns received from a flight simulator, external to the platform. The platform, due to its moving parts, is subjected to the Machinery Directive.

However, due to the complexity of motion profiles of such systems, following current functional safety standards result in a poor PL classification, due to the low PFH value reached. This low PFH value is due to the pessimistic estimation proposed by the ISO 13849, as all the 6 axes are considered simultaneously.

[1] In chapter 4, the pressure mat and the safety relay are components that are designed to "supply" a safety function, with a PL rating and PFH value.

[2] Motion cue is illusion of movement for the human sensory system.

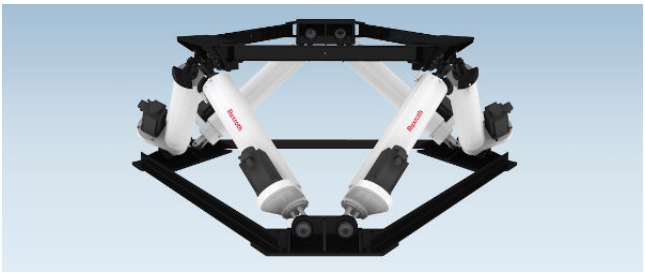

Figure 37 – Motion simulation platform built by Bosch Rexroth.

In this context, intention of Bosch Rexroth is to adapt its products to the Machinery Directive, as well as train people to understand and know how to design to following safety rules, laws, regulations and requirements.

To comply with the mentioned objectives, the office in Boxtel, the Netherlands, responsible for design and manufacture of motion platforms, started a project for study of functional safety in motion simulation systems. Objectives of this project are:

1. Improve documentation for the Machinery Directive;
2. Qualification building program for system designers;
3. Design integrated safety functions to facilitate integration to complete systems;
4. Achieve better PL through more accurate PFH.

Methods proposed in chapter 3 of this work has direct application to this project.

5.1 SYSTEM DESCRIPTION

A complete flight simulator consists of motion and visual simulation systems, in a replica of the control panel of a specific aircraft, as well as a simulation software that calculates response of aircraft to the controls.

Bosch Rexroth does not deliver complete flight simulators. Scope of supply consists of:

- 6 DOF motion platform;

- Cables;
- Control cabinet;
- Motion computer, that calculates inverse kinematics for the actuators.

It is intended for system integrator, that will add a cabin with visual system and control panel. The cabin mimics a specific aircraft, and is normally built to a specific customer. For an application, it is still necessary to add cabin, simulation software and surroundings installation, like fences and access means and safety sensors.

5.2 PROJECT DESCRIPTION

In order to achieve the desired goals, a proposal of activities for the project is made. Each activity is discussed briefly in the following sections.

5.2.1 Analysis of legal requirements

Depending on the intended market, different regulations must be considered. The objective of the analysis is to identify which regulations must be considered. In the case of Europe, Machinery Directive is mandatory, and local requirements may apply depending on the country. In Brazil, products must fulfill requirements of Norma Regulamentadora 12.

Inputs: Intended market.
Requirements: Knowledge about legal requirements.
Outputs: List of regulations.

5.2.1.1 Classification under Machinery Directive

A product may be classified as machinery or partly completed machinery under the Machinery Directive (see appendix A). This classification impacts in the necessary documentation and even in the approval of the machinery.

Inputs: None.
Requirements: Knowledge on the Machinery Directive.

Outputs: Decision of a product is classified whether as machinery or partly completely machinery.

5.2.2 Identification of the state of the art in the technology

Identification of what is expected in terms of safety. This is accomplished by comparison of similar products in the market, and also by the available solutions. Some standards, in some countries, have also normative requirements that must be taken into account.

Inputs: Intended market.

Requirements: None.

Outputs: Typical solutions available and typical required PL or SIL for reference.

5.2.3 Identification of applicable standards

Inputs: None.

Requirements: Knowledge about standards.

Outputs: List of standards that may provide technical solutions

5.2.4 Risk assessment

Risk assessment should be performed according to ISO 12100 for the machinery sector. As it is a comprehensive activity, it is subdivided in other activities, that are detailed in the following subsections.

5.2.4.1 Description of the system

It is necessary for the team to identify which tasks are performed on the system, during the whole life cycle. Therefore, not only designers, but also end users and maintenance personal must be involved.

Inputs: None.

Requirements: A multidisciplinary team that involves end users, assembly and maintenance personal and designers.

Outputs: A comprehensive description of the system

5.2.4.2 Identification of tasks during whole life cycle

It is necessary for the team to identify which tasks are performed on the system, during the whole life cycle. Therefore, not only designers, but also end users and maintenance personal must be involved.

Inputs: Specifications, system description and preliminary concept of the machinery, when available.

Requirements: A multidisciplinary team that involves end users, assembly and maintenance personal and designers.

Outputs: A comprehensive description of the system

5.2.4.3 Identification of physical limits of machinery

This activity is basis for assignment of severity of hazards. It is also basis for the operational limits, which must be in the documentation.

Inputs: Specifications, system description and preliminary concept of the machinery, when available.

Requirements: A multidisciplinary team that involves end users, assembly and maintenance personal and designers. Selection of a multidisciplinary team is further discussed in section 5.2.7.

Outputs: Definition and documentation of the limits of the machinery.

5.2.4.4 Identification of hazards

This task consists in understanding how an accident occurs and to describe it systematically, in terms of source, events, life phase and nature of the hazard.

Inputs: Annex B of ISO 12100. Other hazards lists from other standards (specially C-type standards) provide an improved process.

Requirements: A copy of each standard.

Outputs: A list with all hazards occurring in all life phases.

5.2.4.5 Risk estimation

Assignment of risk parameters for each hazard, in order to prioritize risks to be reduced and to quantify the amount of risk reduction.

Inputs: A list with all hazards occurring in all life phases.
Requirements: None.
Outputs: A list with a risk number for each hazard.

5.2.4.6 Risk evaluation

The decision whether a risk is acceptable or not is based on the state of the art and on internal guidelines of the company;
Inputs: A list with all hazards occurring in all life phases, each with a risk number.
Requirements: Comparison with existing solution and internal guidelines.
Outputs: Decision to reduce risk associated to a hazard.

5.2.5 Design of safety function

For the hazards whose risk is not possible to be reduced by inherently safe design, safeguards and protective measures may be used. If these measures rely on a control system, they shall be designed according to ISO 13849. Following the *10 Steps to Performance Level* methodology (ORTH et al., 2012) helps to design safety functions. Nevertheless, adoption of methods from chapter 3 of this work requires additional steps. These additional steps are detailed in the following sections.

5.2.5.1 Specify which hazards to reduce risks with each safety function

A single safety function may reduce risks associated to different hazards. An analysis of which safety function reduces which risks is necessary to quantify how much each risk is reduced, and whether further risk reduction is necessary
Inputs: Risk assessment.
Requirements: None.
Outputs: A cross-correlation list of safety functions and hazards.

5.2.5.2 Define functional requirements for safety functions

Description of reaction times, in which operation mode each function is active, priority of each function and behavior in case of failures. The *10 Steps to Performance Level* methodology is recommended for that, together with applicable C-type standards.

Inputs: Concept of each safety function.

Requirements: Output of activity 2 (state of the art) and activity 3 (applicable standards).

Outputs: Detailed description of each safety function.

5.2.5.3 Define required PL of each safety function

Definition of the required PL of each safety function based of the required amount of risk reduction. The amount of risk reduction is defined in risk assessment, activity 4.

Inputs: Risk assessment (activity 4).

Requirements: Output of activity 2 (state of the art) and activity 3 (applicable standards).

Outputs: The required PL of each safety function.

5.2.5.4 Design of the safety circuit

As the machinery has already a preliminary concept, with circuits for the realization of functions, it is possible to analyzed how the safety reaction must act and design it, adding components if necessary. Together with design, it is necessary to build a reliability model of the safety function. Failure detection and tests must be specified as well.

Inputs: Schematic circuits of the machinery.

Requirements: Knowledge in design for functional safety, knowledge in standards and knowledge in system reliability modeling techniques.

Outputs: Updated schematics with safety related components, proportion of detected failures and description of tests.

5.2.5.5 Obtain field failure data for components

Field failure recordings must be available for the intended application.

Inputs: List of safety related components.

Requirements: Availability of records of field failure data. The company must implement a culture of surveillance of products.

Outputs: Field failure recordings.

5.2.5.6 Derive failure parameters from field data

From the recordings, it is necessary to fit data to a failure distribution.

Inputs: Field failure recordings.

Requirements: Knowledge in reliability analysis.

Outputs: Failure parameters for each component.

5.2.5.7 Calculation of PFH according to methods of chapter 3

Application of methods from chapter 3 and illustrated in chapter 4.

Inputs: Reliability model of the safety function (activity 5.4), failure parameters (activity 5.6) and proportion of detected failures (activity 5.4).

Requirements: Knowledge in system reliability and functional safety.

Outputs: Estimate of PFH.

5.2.5.8 Verification of PL

Proof check of PFH calculation, verification whether the qualitative requirements are fulfilled and if the achieved PL is equal or higher than the required.

Inputs: Calculation of PFH, safety standards.

Requirements: Knowledge in functional safety and in the machinery.

Outputs: Decision whether the safety function meets the required PL or has to be redesigned.

5.2.5.9 Testing of safety function for validation

Testing in a prototype whether the safety reaction is suitable, in terms of the functional requirements, and check for unforeseeable conditions.

Inputs: Detailed description of safety functions (activity 5.2).

Requirements: Existing prototype.

Outputs: Decision whether the safety function meets the functional requirements.

5.2.5.10 Verification of achieved risk reduction

The required risk reduction, specified in the risk assessment, must be checked.

Inputs: Designed safety function.

Requirements: Multidisciplinary team.

Outputs: Decision whether risk reduction provided by safety function is enough.

5.2.6 Preparation of documentation

For compliance to the Machinery Directive, external and internal documentation must be created. It is strongly recommended that each individual activity is documented as they are executed, facilitating this last activity.

5.2.7 Team definition

A multidisciplinary team is necessary for designing of a machinery and compliance to safety regulations. This is necessary in order to understand how the machinery interacts with people during its whole life cycle, from conception until disposal. It is not necessary to assign an employee for each of the points listed below, nor that all assigned are present in every activity. However, it should be avoided to assign only one employee for the whole process.

Knowledge necessary for the project:

- Knowledge in the technical system, to design solutions;

- Knowledge in assembly, maintenance, commissioning, to identify tasks and interaction of employees and machinery;
- Knowledge in risk assessment for moderation of meetings;
- Knowledge of requirements and regulations;
- Knowledge of system reliability modeling methods.

In order to apply the proposed method, it is necessary to have more accurate failure data. Such data is normally not available. For some companies, it is possible to perform an analysis of field failure of similar applications, in order to obtain the failure data. For this case it is necessary:

- Collection of field failure data;
- Knowledge of reliability analysis to calculate failure parameters;

5.3 IMPLEMENTATION

Due to organizational factors at Bosch Rexroth, was not possible to conclude all activities of the project during the assigned time at Boxtel. To the time of conclusion of this work, the project reached the definition of safety function phase (activity 5.2). Results up to this phase are presented in the following sections.

5.3.1 Classification under the Machinery Directive

It is clear that the motion platform is intended to used with a cabin with visual system and control panel, what gives an impression of partly completed machinery. However, it is possible to install only the delivered equipment and generate hazardous movements by the manual operation mode. As it could generate hazardous movements by itself, it could be regarded as a machinery.

The important point of classifying as a machinery implies compliance with all applicable health and safety requirements from the Annex I from the Machinery Directive.

The platform makes hazardous movements, which are controlled by its own control system and by external equipment. Therefore, requirements over mechanical hazards and hazardous situations generated by the control system are applicable.

Due to the scope of delivery, the system does not allow compliance with some of the applicable requirements of Annex I. They are listed below:

- Annex I, item 1.2.1. *the protective devices must remain fully effective or give a stop command* (EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION, 2006). As a risk reduction measure, it is recommended that protective devices are used, like fences. These protective devices may have interlocks, to give stop command to the system. However, as they do not make part of the delivery, compliance with the item cannot be assured.

- Annex I, item 1.3.9. Risk of uncontrolled movements. It is not possible to ensure that the platform will not move uncontrollably, as the control signals come from external parts.

This is represented in figure 38. While it is possible to design the logic and output sub-functions of the safety function, input relies on sensors which are not part of the delivery. Therefore, it is not possible to ensure, for Bosch Rexroth, that the control system of the motion platform fulfills all applicable EHSR.

Based on the argumentation above, the motion simulator has to be regarded as partly completed machinery according to the European Machinery Directive 2006/42/EC.

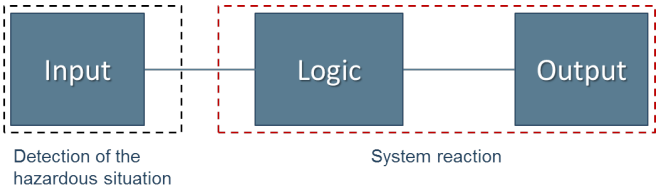

Figure 38 – Architecture of safety functions for motion platforms. Logic and output sub-functions can be realized within the scope of the deliver; input sub-function not.

Classification of the motion simulation system as partly completed machinery impacts in the work flow for compliance to the Machinery Directive. Based on appendix A, it becomes as represented in figure 39.

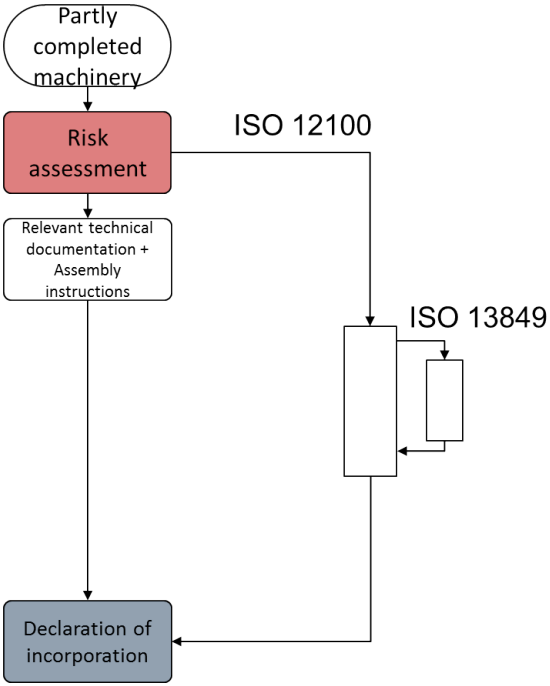

Figure 39 – Overview of activities for compliance to the Machinery Directive

5.3.2 Risk Assessment

Risk assessment was the most time consuming part of the project due to its scope. Annex B of ISO 12100 and Annex A of ISO 10218-1 were used to identify and describe hazards. Risk parameters were assigned to each hazard, and risk reduction measures were discussed.

5.3.3 Safety functions

For mechanical hazards that arises from uncontrolled movements, safety functions were suggested:

- Maintenance position;
- Displacement limit of each actuator;

- Safety-related stop;
- Avoidance of unexpected start-up;
- Speed limitation in special mode.

A discussion about applicability of the method and the activities follows in the conclusion chapter.

List of Activities:

Activity 1 - Analysis of legal requirements;
- Activity 1.1 - Classification under Machinery Directive;

Activity 2 - Identification of the state of the art in the technology;

Activity 3 - Identification of applicable standards;

Activity 4 - Risk assessment;
- Activity 4.1 - Description of the system;
- Activity 4.2 - Identification of tasks during whole life cycle;
- Activity 4.3 - Identification of physical limits of Machinery;
- Activity 4.4 - Identification of hazards;
- Activity 4.5 - Risk estimation;
- Activity 4.6 - Risk evaluation;

Activity 5 - Design of safety function;
- Activity 5.1 - Specify which hazards to reduce risks with each safety function;
- Activity 5.2 - Define functional requirements for safety functions;
- Activity 5.3 - Define required PL of each safety function;
- Activity 5.4 - Design of the safety circuit;
- Activity 5.5 - Obtain field failure data for components;
- Activity 5.6 - Derive failure parameters from field data;
- Activity 5.7 - Calculation of PFH according to methods of chapter 3;
- Activity 5.8 - Verification of PL;
- Activity 5.9 - Testing of safety function for validation;
- Activity 5.10 - Verification of achieved risk reduction;

Activity 6 - Preparation of documentation;

6 CONCLUSION

In this chapter, the develop methods, their importance, applicability and limitations are discussed. At the end, suggestions for further development in this field.

6.1 IMPORTANCE

Functional safety in the machinery sector has the objective of reducing the number of work accidents and strive for health and safety of employees. Regulations arose from this society demand, and increase complexity of machinery design. Quantification of PFH is regarded as a complex subject. In one hand, methods are difficult and simplicity is necessary. The effort for small companies to build detailed reliability models for a one-time design machine is burdensome. In the other hand, calculations are not accurate, due to the restrictive hypothesis used for modeling safety function as Markov processes.

What seems to be a dilemma has a common solution. Development of sub-modules with integrated safety functions facilitates engineering effort for small companies. Such sub-modules are not one-time design, what justifies more effort in engineering, as in the case of the motion simulation system.

This work addressed an open point in research of functional safety, which is consideration of more accurate failure models for pneumatic, hydraulic and electromechanical components. Failure of such components occur mostly due to aging mechanisms, e.g. wear-out and corrosion, being concentrated at the end of product life. Models with constant failure rate underestimate the average frequency of dangerous failure per hour (PFH).

This work follows the line of works from Bosch Rexroth (refer to section 1.6), being a sequence for Orth and Raksch (ORTH; RAKSCH, 2014). There, use of Weibull distribution is suggested, but for derivation of an Mean Time To dangerous Failures ($MTTF_d$) value. This present work enables usage of Weibull distribution, as proposed by Orth and Raksch, directly for calculation of PFH for machines with hydraulic control systems.

The objective proposed in section 1.8 was reached, with limitations. A method for calculation of PFH, comprising modeling of the safety function in reliability block diagrams (RBD) and discrete event

simulation was proposed in chapter 3. In section 3.5 and in appendix E, it is shown that the proposed method leads to similar results as simplified method for PFH estimation of ISO 13849, for categories B, 1, 3 and 4. In section 3.6, Weibull distribution for failure of components of a safety function is added to proposed method, also for categories B, 1, 3 and 4. In section 3.6 and in chapter 4, effects of Weibull distribution on PFH of a safety function are analyzed. As a further advantage of proposed method, it provides that capability of calculating PFH for different mission times (different from 20 years).

Limitations of proposed method are due to assumptions made to derivation of equations 3.16 to 3.25, presented in section 3.6 and appendix D. The strongest and most limiting assumption is the same shape factor β_W for all failure modes, dangerous and safe. This assumption is intended to supersede limitations of input data, which come from field failure analysis (Weibull analysis). Availability of field failure data is a limitation *per se*. Another limitation is related to derivation of equations for block E, which were derived numerically.

Suggestions for overcome such limitations include access to more detailed failure data, which enables to generate failure distribution from field data analysis for each block individually. An exhaustive Failure Modes and Effects Analysis (FMEA) to derive accurate values for Diagnostic Coverage should be carried, to complement failure data. Due to the high costs in development, it may not be suitable for small machine builders and for one time designs. Additionally, percentage of common cause failures (β_{CCF}) has to be better estimated.

As sub-products of this work, there are other contributions:

- Clarification of the meaning of PFH: There is a common misunderstanding in the machinery sector regarding reliability, availability, risk and PFH. An attempt to clarify differences and relations of reliability and PFH is made through appendix B and section 3.4. Additionally, appendix B is intended to clarify that PFH is a measure for repairable systems (refer to section sec:reliability), and shall not be mistaken with Mean Time To Failure (MTTF), which is a measure for non-repairable systems.

- ISO 13849 is still not valid in Brazil. The current standard for safety of machine controls is ABNT 14153, which is the national counterpart of EN 954 (refer to section 1.4.1). This situation is however to change. In 2010, the *Norma Regulamentadora 12* (NR12) was reformulated, becoming closer to the Machinery Directive 2006/42/EC (refer to appendix A. ISO 12100 was adopted

as a national standard as ABNT ISO 12100 in December of 2013. As it is part of framework of risk reduction of the Machinery Directive, ISO 13849 is expected to be adopted as a national standard. In order to promote application of ISO 13849 in Brazil, this work generated the publication: I. R. Kuhlhoff, U. F. Moreno, and A. Orth. "Aplicação da Norma ISO 13849 de Segurança Funcional de uma bancada de testes hidráulica". Congresso Brazil Automation 2014. São Paulo/SP - Brazil. (KUHLHOFF; MORENO; ORTH, 2014), with basics of the standard and a case study.

- A fist attempt to integrate functional safety activities and engineer projects is made in chapter 5.

6.2 SUGGESTION FOR FUTURE WORKS

Proposed method achieved calculation of PFH with Weibull distributed failures, but with strong limitations. The method can be however adapted, by changing equations of step 3 of method presented in section 3.4.

Legal requirements and modeling of category 2 of ISO 13849 are still poorly understood. A deeper investigation is required, to understand how to model effects of periodic tests, its relation with demand and what is normative by the standard.

Common cause failures are regarded as one of the most impacting factors in quantification of systems with high reliability. The Beta-factor model, while simple, may be conservative. For systems with more than two channels, the Beta-factor model is not recommended (GOBLE, 2010). Therefore, a study of other models for estimation of CCF are necessary for systems aiming high Performance Level (PL) or Safety Integrity Level (SIL) values.

Estimation of PFH considers only physical failures of components. A study of the impact of systematic failures is necessary, in order to understand how it affects the quantification of PL.

APPENDIX A – Framework for safety of machinery

Functional safety in the machinery sector belongs to a framework for machinery safety. In this section, the basis of this framework is explained.

A.1 EUROPEAN MACHINERY DIRECTIVE 2006/42/EC

For Europe, the Treaty on the Functioning of the European Union regulates aspects common aspects for the European Union, such as safety regulations. From the Treaty, there are Directives that place requirements on markets, that must be adopted as law by its country members. In the field of machinery, there is the European Machinery Directive 2006/42/EC that regulates the machinery market, putting restrictions and requirements on machinery, regulating the internal market and the social safety protection of employees.

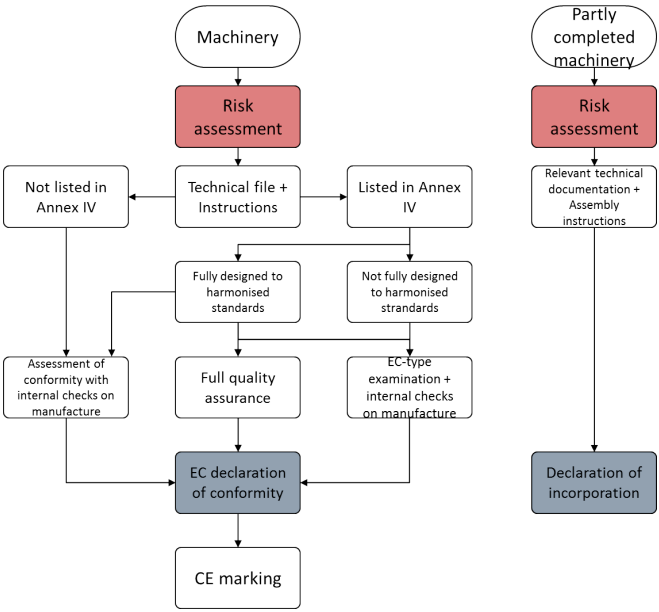

Figure 40 – Work flow for implementation of Machinery Directive for machinery and partly completed machinery. Adapted from the Guide for the Machinery Directive(GUIDE..., 2010) and Orth(ORTH et al., 2012).

In order to be sold and commercialized in Europe, machinery

must have the **CE mark** affixed to it. The mark is affixed by the manufacturer, who must prove that machinery fulfill the **Essential Health and Safety Requirements, EHSR**, which strive for the protection of employees.

The Machinery Directive was made in order to ensure safety of users, during all the life cycle of machinery, as well as for all machinery. To cover all the cases, it has an abstract structure and additional requirements for different types of products.

One of the innovations of the Machinery Directive is that it coined the term **partly completed machinery**. It is a denomination that is intended to cover subsystem and modules that, although cannot fulfill a function and therefore are not directly commercialized to end users, they are sold and incorporated in bigger machines. As such subsystem may pose hazards as well due to design and manufacturing problems, its manufacturer is made responsible by the Machinery Directive.

The Directive applies to: machinery; interchangeable equipment; safety components; lifting accessories: chains, ropes and webbing; removable mechanical transmission devices and partly completed machinery. All of them are classified as machinery, except for the partly completed machinery. In that way, a product can be classified either as:

- **machinery**: *an assembly, fitted with or intended to be fitted with a drive system other than directly applied human or animal effort, consisting of linked parts or components, at least one of which moves, and which are joined together for a specific application* (EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION, 2006), or
- **partly completed machinery**: *means an assembly which is almost machinery but which cannot in itself perform a specific application. A drive system is partly completed machinery. Partly completed machinery is only intended to be incorporated into or assembled with other machinery or other partly completed machinery or equipment, thereby forming machinery to which this Directive applies* (EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION, 2006).

According to the classification of a product under the Directive, it has different requirements and work flow, different documents and shall or shall not receive the CE marking. These different work flows, technical documentation are represented in figure 40.

The Machinery Directive define a legal framework for safety of machinery. That is, requirements in a abstract level. Standards are support elements that give a technical solution that fulfill all/part of the requirements.

Standards listed in the Official Journal of the European Union[1]are regarded as **harmonised standards**. This denomination means that there is the **presumption of conformity** principle (is valid). The presumption of conformity effect means that once that the standard is applied, the respective EHSR is fulfilled, being not necessary for the builder to prove each individual requirement by its own.

For the machinery directive, there is a well established structure of harmonised standards[2]. This structure is defined by type A, B and C standards.

- ***type-A standards****(basic safety standards) giving basic concepts, principles and general aspects that can be applied to machinery;*
- ***type-B standards****(generic safety standards) dealing with one safety aspect or one type of safeguard that can be used across a wide range of machinery;*
- *type-B1 standards on particular safety aspects (for example, safety distances, surface temperature, noise);*
- *type-B2 standards on safeguards (for example, two-hand controls, interlocking devices, pressure-sensitive devices, guards);*
- ***type-C standards****(machine safety standards) dealing with detailed safety requirements for a particular machine or group of machines;*

When requirements of standards diverge from each other, type-C standards have priority over type-B, which have priority over type-A.

A.2 RISK ASSESSMENT AND RISK REDUCTION - ISO 12100

For the Machinery Directive, it is of most importance to perform a risk assessment. It is used as basis to systematically identify hazards and reduce risks. As represented in figure 40, the red blocks are start of

[1] http://eur-lex.europa.eu/oj/direct-access.html

[2] URL for MD harmonised standards: http://ec.europa.eu/enterprise/policies/european-standards/harmonised-standards/machinery/index_en.htm

risk assessment process, whose results are necessary for the blue blocks, proving that the EHSR are fulfilled.

ISO 12100 standard is a A-type harmonised standard. It describes a systematic risk assessment work flow for the machinery sector. It consists of five steps (International Organisation for Standardization, 2010):

1. Determine the of limits of the machinery, including the intended use and any reasonably foreseeable misuse;
2. Identify of hazards and associated hazardous situations;
3. Estimate the risk for each identified hazard and hazardous situation;
4. Evaluate the risk and decision taking about the need for risk reduction;
5. Elimination of the hazard or reduce the risk associated with the hazard by means of protective measures.

The standard provide guidance for each step. Annex B has a list of hazards and hazardous situations, helping designers to identify and describe them in a organized way.

Risk reduction, as recommended by ISO 12100, consists of adopting 3 hierarchical steps. They are:

1. Inherently safe design measures;
2. Safeguarding and/or complementary protective measures;
3. Information for use.

The reason for this prioritization is the effectiveness of the measures. More effective measures shall be applied first, aiming at removing unnecessary hazards, and just then are applied measures to reduce frequency of occurrence of accidents by safeguarding and information.

For each of the risk reduction steps, other standards are suggested, for specific types of hazards or protective measures. For example, ISO 13857 is recommended for gaps between moving parts, avoiding that body parts can enter in it; ISO/TR 11688-1 is recommended for reduction of noise emission.

For safeguarding measures that rely on a control system, ISO 13849 is suggested for the design of the safety-related control system. Figure 41 represents graphically this relation. From the risk assessment comes input information necessary for design, and output of ISO 13849 design process returns for ISO 12100 in order to check if risk reduction is achieved.

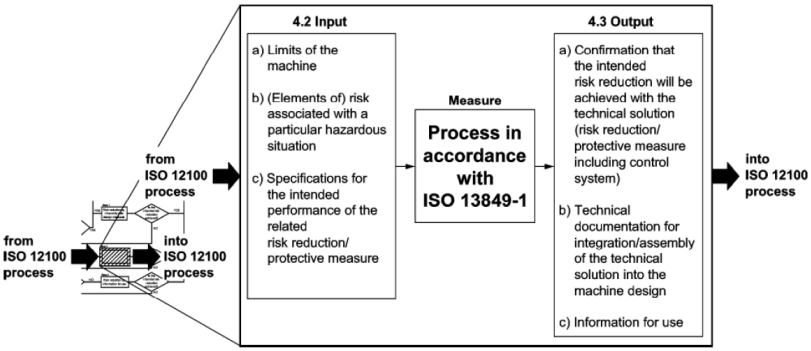

Figure 41 – Relation of ISO 13849 to ISO 12100. Extracted from ISO/TR 22100-2 (International Organisation for Standardization, 2013).

A.3 FUNCTIONAL SAFETY IN THE MACHINERY SECTOR - THE ISO 13849

ISO 13849 standard is a B1-type harmonised standard. Risk assessment and reduction is defined by ISO 12100, whereas ISO 13849 define design procedures and requirements for one specific kind of risk reduction measures. Compliance to ISO 13849 is important, however not enough to guarantee a safe machine.

Difference of scope of standards is represented in figure 42.

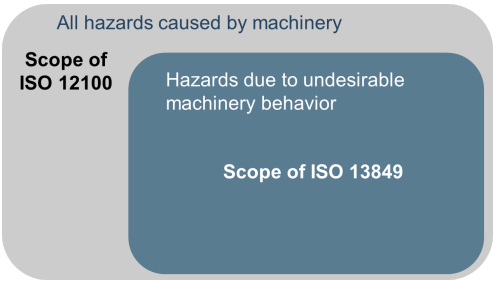

Figure 42 – Scope of ISO 12100 compared to ISO 13849

Considering the ISO 12100 and the ISO 13849 standards in the Machinery Directive, the work flow figure can be update, as in figure 43. The methodology *10 Steps to Performance Level*(ORTH et al., 2012) is recommended for compliance with ISO 13849.

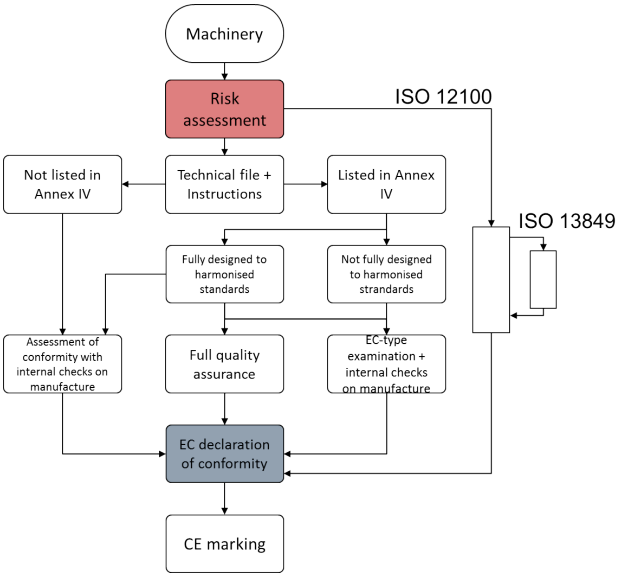

Figure 43 – Updated work flow for compliance with Machinery Directive, considering ISO 12100 and ISO 13849 standards.

A.4 BRAZILIAN FRAMEWORK FOR MACHINERY SAFETY

In Brazil, machinery must comply to the **Norma Regulamentadora 12, NR12** for short, which is adopted as law. The NR12 pose health and safety requirements in machinery, in order to provide a safe workplace for employees and user. Its last major review in 2010 (MINISTERIO DO TRABALHO E EMPREGO, 2013) assigned a bigger responsibility to machine builders and designers, that must prove that machinery is safe in the whole life cycle. It defines also that old machines must be adapted to new requirements.

The NR12 assign some standards that are mandatory, in order to ensure safety of machinery. Standards adopted are issued by the Brazilian Association for Technical Standardization, the **Associação Brasileira de Normas Técnicas, ABNT**. The ABNT, as a member of the **International Organization for Standardization, ISO**, is in process of adoption of ISO standards.

APPENDIX B – Intuitive interpretation of PFD_{avg} and PFH

PFD_{avg} and PFH are characteristic of the safety function, which quantify the incidence of potential accidents caused by dangerous failure of the components. Functional safety standards determine it through reliability of components. Nevertheless, it still relates to other characteristics, as detection of failures and demand of function. The difference between PFD_{avg} and PFH depends on these characteristics. In the following pictures, an interpretation for PFD_{avg} and PFH is given, in a system's perspective. Even that PFD_{avg} is not used in the machinery sector, it is important to understand the difference between the two concepts, to avoid misunderstanding.

It is assumed that demands are instantaneous, i.e. a demand has no duration, or very short duration that it can be regard as instantaneous. The reason for that is that demands in the machinery sector are short in relation to mission time.

Another important point is that safety functions are *repairable*. In the event of a failure, the safety function must be repaired, to maintain the safe operation. This is achieved by changing failed components. Components fail and are replaced. Control systems fail and are repaired through replacement of components. Therefore, both PFD_{avg} and PFH reflect this characteristic of repair.

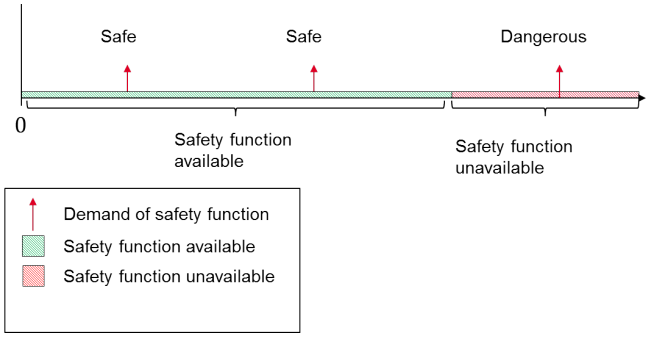

Figure 44 – Demand of safety function in different system conditions

The hypothetical situation of figure 44 represents a hazardous situation that is intended to be reduced or avoided. In the time frame of one year, there is the time where the safety function is available and some time that it is not, that is, it has failed without notice. A demand represents a dangerous event which has been made safe through the reaction of the control system. However, after some time, the safety function fails unnoticed, and a further demand is not made safe.

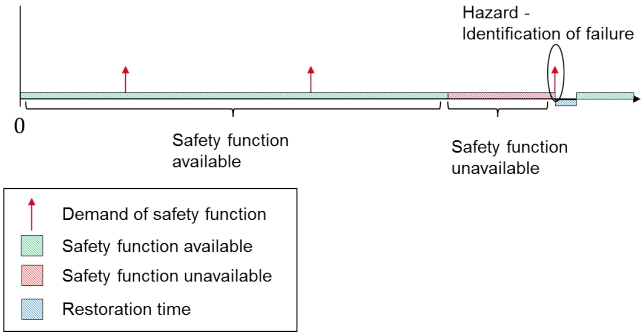

Figure 45 – Demand as a failure identification process

In the case of figure 45, it can be seen that the demand, apart from the possibly bad consequences, also reveals the dormant failure of the control system. In this case, after the failure has been detected, the safety function can be restored to functioning. The proportion of time that the safety function remains unavailable to the total time is a reliability metric of safety systems, called PFD. PFD stands for *probability of failure on demand*, and can be interpreted as:

$$\boldsymbol{PFD_{avg} = \frac{MDT}{MUT + MDT}} \tag{B.1}$$

Where MDT means *Mean Downtime* and MUT means *Mean Uptime*.

The higher the downtime proportion to the total time, the higher the probability of a random demand occur in a time that the safety function is unavailable. This proportion is what is desired to be reduced in the design of a safety control system.

In the case that the demands are much more frequent, as in the figure 46, failures do not stay much time in the failed state. That is, after a failure has occurred, it will be probably discovered soon. This drastically reduces the proportion of unavailable time of the safety function to the total time. In the limit, when the demands are continuous, the downtime of each failure collapses to the restoration time[1].

Using the $\mathrm{PFD}_{\boldsymbol{avg}}$ for evaluating the integrity of the safety function in this case may cause false impressions. Even that the $\mathrm{PFD}_{\boldsymbol{avg}}$ will become much lower, it is due to the high demand. That is, the downtime is lower, but the likelihood of an accident remains the same. Measuring the proportion of the downtime in this case becomes mislead-

[1] which is many orders of magnitude lower than the uptime, being close to zero

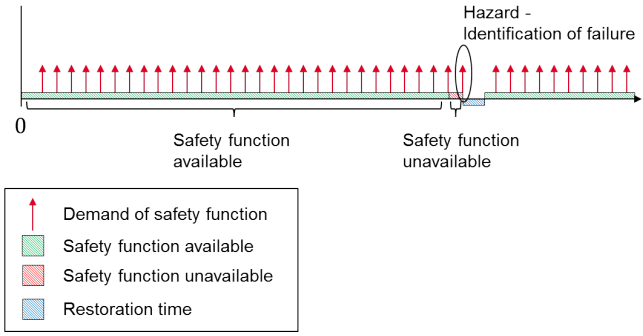

Figure 46 – Increase in demand rate causes the failures to be identified sooner

ing. The downtime becomes much smaller, giving the false impression of an increase of safety integrity. Users may think that the hardware has increase ability to withstand dangerous failures. But what really happens is that failures are detected faster due to the high demand, leading to smaller times with dormant (non-detected) failures.

Therefore, a different measure is need to evaluate this case. It is used the PFH, the average frequency of failure, which can be interpreted as:

$$\boldsymbol{PFH = \frac{N(t)}{MUT + MDT} = \frac{N(t)}{Totaltime}} \tag{B.2}$$

Where $\boldsymbol{N(t)}$ is the number of times that the safety function fails in a dangerous mode.

In the limit case that the downtime of each failure collapses to zero[2], the transition of being available to unavailable can lead to an accident and this measure is assessed[3].

To reduce *de facto* the incidence of failures, other measures have to be taken. Figure 47 a situation closer to reality. In order to reduce incidence of dangerous failures leaving the system without protection, failure detection capability is added to the safety function. Dangerous failures detected before a demand occurs do not count to calculation of PFH, therefore reducing it.

This difference in PFD and PFH reflects also in the failure modes which are more relevant for each case. In PFD, with low-demand, the

[2]if the restoration time is zero

[3]This is the *continuous operation mode* of the IEC 61508

system remains static for a long time, what makes it prone to failure modes as corrosion, deposit, sticking, etc. In PFH systems, functions are prone to fatigue and wear failure modes, as abrasion, friction, etc.

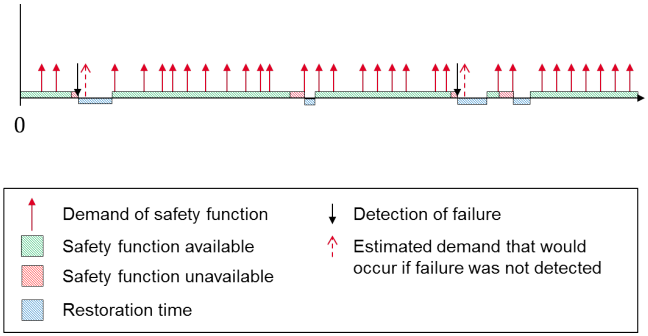

Figure 47 – Use of on-line tests to reveal failures before a demand occurs

From the figures 44, 45, 46 and 47 and the related explanation, an intuitive idea of PFH was built. This interpretation is used in chapter 3 for setting up simulation parameters.

APPENDIX C – Deduction of equation for the number of simulations

This section is dedicated to deduct equation 3.2, for determination of the number of simulation needed to achieve the required precision for PFH.

The higher the safety requirements, the lower frequency of failures is tolerable. Therefore, it must be shown that the components reach a very low frequency of failure.

In order not to allow numeric errors in the computation of PFH through simulation, it is necessary to determine the minimum number of runs that is needed to achieve such low PFH.

PFH is calculated through expected number of failures, as equation 2.29.

BlockSim calculates the expected number of failures by averaging the number of failures. That is, if 1000 runs are made, the number of failures is counted and divided by 1000 (number of runs).

Each run can be viewed as a Poisson process.

Let N(t) be a counting process. Each time a failure of the safety function occurs, N(t) is incremented by 1. N(t) denotes the number of failures in each run.

The expected number of failures E(N(t)) is obtained estimated by averaging the number of failures N(t) for each of the N runs, for the time point t.

$$\hat{\boldsymbol{E}}(\boldsymbol{N}(\boldsymbol{t})) = \frac{\mathbf{1}}{\boldsymbol{N}} \sum_{\boldsymbol{i}}^{\boldsymbol{N}} \boldsymbol{N_i}(\boldsymbol{t}) \tag{C.1}$$

Where $\hat{\boldsymbol{E}}(\boldsymbol{N}(\boldsymbol{t}))$ is an estimate for the expected number of failures at time $\boldsymbol{t}$, N is the number of simulations and $\boldsymbol{N_i}(\boldsymbol{t})$ is the number of failure of the simulation/run $\boldsymbol{i}$ at time $\boldsymbol{t}$.

It is important to note that the domain of $\boldsymbol{N_i}(\boldsymbol{t})$ is the set of natural numbers $\mathbb{N}$, while the domain of $\hat{\boldsymbol{E}}(\boldsymbol{N}(\boldsymbol{t}))$ is the set of non-negative real numbers $\mathbb{R}_{\mathbf{0}}^{+}$.

The smallest non-zero number that $\boldsymbol{N_i}(\boldsymbol{t})$ can assume is 1. As N is finite, the smallest number that $\hat{\boldsymbol{E}}(\boldsymbol{N}(\boldsymbol{t}))$ can reach is determined by N. As the number of failures increases, $\hat{\boldsymbol{E}}(\boldsymbol{N}(\boldsymbol{t}))$ also increases, always by an increment of $\mathbf{1}/\boldsymbol{N}$.

Let $\boldsymbol{\epsilon_N}$ denote the increment $\mathbf{1}/\boldsymbol{N}$. Substituting the $\hat{\boldsymbol{E}}(\boldsymbol{N}(\boldsymbol{t}))$ in equation 2.29 results in

$$\frac{\mathbf{1}}{\boldsymbol{T_M}} \hat{\boldsymbol{E}}(\boldsymbol{N}(\boldsymbol{T_M})) = \frac{\mathbf{1}}{\boldsymbol{T_M}} \boldsymbol{\epsilon_N} \tag{C.2}$$

which is the smallest increment for PFH, denoted as $\boldsymbol{\epsilon_{PFH}}$. It is a function of the mission time and the number of simulations.

Rewriting equation C.2 in terms $\boldsymbol{\epsilon_{PFH}}$, N and $\boldsymbol{T_M}$ leads to

$$\boldsymbol{N = \frac{1}{\epsilon_{PFH} \cdot T_M}} \tag{C.3}$$

PFH values in table K.1 from ISO 13849 are represented in scientific notation, with two decimal places. The $\boldsymbol{\epsilon_{PFH}}$ of the calculated PFH is desired to be of one order of magnitude lower than the second decimal place, or alternatively, 3 orders of magnitude lower than the target PFH value. That is:

$$\boldsymbol{\epsilon_{PFH} = 10^{-3} \cdot PFH_{target}} \tag{C.4}$$

Substituting equation C.4 in C.3

$$\boldsymbol{N = \frac{1}{10^{-3} \cdot PFH_{target} \cdot T_M}} \tag{C.5}$$

From equation C.3, it can be seen that precision of PFH calculation is dependent of the increment $\boldsymbol{\epsilon_{PFH}}$ and the mission time $\boldsymbol{T_M}$. Therefrom arises an effect of compromise: the lower the mission time to be considered, the higher has to be the number of simulations. This conclusion is based on absolute values of $\boldsymbol{\epsilon_{PFH}}$ and $\boldsymbol{T_M}$. Consideration of Weibull distribution with $\boldsymbol{\beta_W}$ higher than one[1]makes failure to happen more concentrated to the end of mission time, with fewer failures at the beginning of the mission time. To compensate this effect, it is necessary to increase further the number of simulations.

[1]shape factor $\boldsymbol{\beta_W}$ higher than one means that failures concentrate in the end of lifetime; this effect increases as the $\boldsymbol{\beta_W}$ increases.

APPENDIX D – Deduction of equations for failure parameters of the 5-block model

Figure 48 – Block diagram of a series system with two blocks

In this model, each block does not represent a single component. Blocks model rather failure modes of a component. However, reliability data is available only to components, and not to its individual failure modes. Parameters of failure distribution for each block are derived from the failure distribution parameters of the components. The parameters diagnostic coverage (DC) and common cause failures factor ($\boldsymbol{\beta}$ -factor model) are used to split the percentage of failures according to each failure mode. The basis hypothesis is that all failure modes have the same shape factor ($\boldsymbol{\beta}$ of the Weibull distribution), and that it is possible to adjust the characteristic lifetime ($\boldsymbol{\eta}$ of the Weibull distribution) to correspond to the percentage of failures. This is based on the theorem below.

D.1 THEOREM

A 2-parameteric Weibull distribution can be decomposed in two other 2-parametric Weibull distributions with the same shape factor ($\boldsymbol{\beta}$) by two fractions summing to one.

D.1.1 Proof

Consider the following system S, with components A and B connected in series, and its reliability block diagram is given in figure 48.

Reliability of a series system is given by:

$$\boldsymbol{R_S(t) = R_A(t) \cdot R_B(t)} \tag{D.1}$$

Let's assume that the reliability function of the system S is known and that it is described by a 2-parametric Weibull distribution.

$$\boldsymbol{R_S(t) = e^{-(\frac{t}{\eta_S})^{\beta_S}}} \tag{D.2}$$

Assume that reliability of components A and B is also described

by a 2-parametric Weibull distribution. So:

$$\boldsymbol{R_A(t) = e^{-(\frac{t}{\eta_A})^{\beta_A}} \quad and \quad R_B(t) = e^{-(\frac{t}{\eta_B})^{\beta_B}}} \tag{D.3}$$

$$\boldsymbol{e^{-(\frac{t}{\eta_S})^{\beta_S}} = e^{-(\frac{t}{\eta_A})^{\beta_A}} \cdot e^{-(\frac{t}{\eta_B})^{\beta_B}}} \tag{D.4}$$

$$\boldsymbol{e^{-(\frac{t}{\eta_S})^{\beta_S}} = e^{-[(\frac{t}{\eta_A})^{\beta_A} + (\frac{t}{\eta_B})^{\beta_B}]}} \tag{D.5}$$

$$\boldsymbol{-(\frac{t}{\eta_S})^{\beta_S} = -[(\frac{t}{\eta_A})^{\beta_A} + (\frac{t}{\eta_B})^{\beta_B}]} \tag{D.6}$$

Assume that the Weibull distribution of both components has the same shape factor as the system's distribution.

$$\boldsymbol{-(\frac{t}{\eta_S})^{\beta_S} = -[(\frac{t}{\eta_A})^{\beta_S} + (\frac{t}{\eta_B})^{\beta_S}]} \tag{D.7}$$

Let

$$\boldsymbol{\eta_A = \frac{\eta_S}{a^{(\frac{1}{\beta_S})}} \quad and \quad \eta_B = \frac{\eta_S}{b^{(\frac{1}{\beta_S})}}} \tag{D.8}$$

Replacing D.8 in D.7

$$\boldsymbol{-(\frac{t}{\eta_S})^{\beta_S} = -[a(\frac{t}{\eta_S})^{\beta_S} + b(\frac{t}{\eta_S})^{\beta_S}]} \tag{D.9}$$

$$\boldsymbol{-(\frac{t}{\eta_S})^{\beta_S} = -[(a+b) \cdot (\frac{t}{\eta_S})^{\beta_S}]} \tag{D.10}$$

Finally:

$$\boldsymbol{1 = (a+b)} \tag{D.11}$$

D.2 DIVISION OF RELIABILITY PARAMETERS

49 represents necessary data for the model, as well as the available data.

From equation D.11 follows that any combination of a and b that sums to one satisfy the hypothesis of a Weibull distribution being decomposable into two Weibull distributions with the same shape factor.

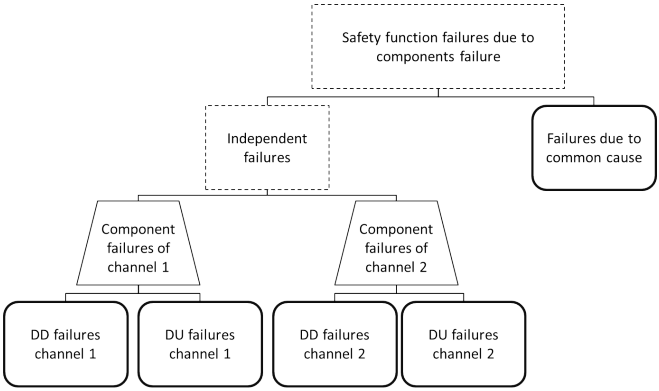

Figure 49 – Division of failures into different failure modes. Trapezoidal form are the available data, rounded rectangles are required data; dashed rectangles are only supporting understanding relations between failure modes.

Choosing $\boldsymbol{a = DC}$ and $\boldsymbol{b = 1 - DC}$ back in equation D.9

$$-(\frac{\boldsymbol{t}}{\boldsymbol{\eta_S}})^{\beta_S} = -[\boldsymbol{DC}(\frac{\boldsymbol{t}}{\boldsymbol{\eta_S}})^{\beta_S} + \boldsymbol{(1 - DC)}(\frac{\boldsymbol{t}}{\boldsymbol{\eta_S}})^{\beta_S}] \tag{D.12}$$

$$\boldsymbol{R_S(t) = e^{-(DC\frac{t}{\eta_S})^{\beta_S}} \cdot e^{-((1-DC)\frac{t}{\eta_S})^{\beta_S}}} \tag{D.13}$$

Reliability of a component is split in two distributions, according to DC. It is possible to calculate an equivalent characteristic lifetime ($\boldsymbol{\eta}$) with D.8. Similar reasoning is applied to common cause failures. For independent DD and DU failures, an additional factor is applied, ($\boldsymbol{1 - \beta_{CCF}}$). Applying it back in D.8

$$\boldsymbol{\eta_A = \frac{\eta_S}{[DC \cdot (1 - \beta_{CCF})]^{(\frac{1}{\beta_S})}}} \tag{D.14}$$

$$\boldsymbol{\eta_B = \frac{\eta_S}{[(1 - DC) \cdot (1 - \beta_{CCF})]^{(\frac{1}{\beta_S})}}} \tag{D.15}$$

For deriving failure parameters for common cause failures, an additional step is needed. The CCF factor is not applied to an individual component failure distribution, but to the whole safety function failure distribution. Therefore, it is necessary to estimate an equivalent

system failure distribution. This equivalent system failure distribution is obtained through BlockSim. A parallel system with input components (trapezoidal forms from 49) is build and failure probability is calculated for various lifetime points. A 2-parametric Weibull distribution is chosen to fit those points. This Weibull distribution assumes $\boldsymbol{\eta_{AUX}}$ and $\boldsymbol{\beta_{AUX}}$. From this distribution, it is possible to calculate parameters for the CCF distribution. Following the condition on the shape parameter:

$$\boldsymbol{\beta_{W,CCF}} = \boldsymbol{\beta_{W,AUX}} \tag{D.16}$$

And, for the characteristic lifetime:

$$\boldsymbol{\eta_{CCF}} = \frac{\boldsymbol{\eta_{AUX}}}{\boldsymbol{\beta_{CCF}}^{(\frac{1}{\boldsymbol{\beta_{W,AUX}}})}} \tag{D.17}$$

APPENDIX E – Analysis of error for validation

E.1 RESULTS VALIDATION METHODS

In order to evaluate the calculation methods, there are some metrics the obtained results. The metrics are presented, percentage error and PFH intervals for a PL.

E.1.1 Percentage error

This measure is calculated by:

$$\boldsymbol{E\%} = \frac{|\boldsymbol{PFH_{calculated} - PFH_{ISO}}|}{\boldsymbol{PFH_{ISO}}} \tag{E.1}$$

The percentage error takes into account the order of magnitude of each quantity.

A weakness of this measures is that there is no reference of what is an acceptable percentage error. A second weakness of this measure is that it does not reflect the division of PL into intervals of PFH. In this sense, an error of 20% may be low, when the reference PFH is in the middle of the interval (e.g. $\mathbf{3 \cdot 10^{-7}}$ [$^{\mathbf{1}}/_{\boldsymbol{h}}$]), but an error of 5% may be prohibitive, when the reference PFH is near the boundaries of other PL interval (e.g. $\mathbf{1.01 \cdot 10^{-7}}$ [$^{\mathbf{1}}/_{\boldsymbol{h}}$]) and leads to a different PL (being too much optimistic about PL estimate).

E.1.2 PFH intervals for a PL

This measure analyzes whether the calculated PFH value reaches the same PL of the reference PFH. No error measure must be calculated.

This measure reflects the intervals characteristic of PL. A disadvantage of this measure is that it may mask errors in calculation, specially systematic errors. Therefore, poor results or poor calculations can be validated, when the result could be easily improved.

E.2 RESULTS OF PFH CALCULATION

E.2.1 Category B or 1

Category B and 1 use the same calculation model. In fact, the difference between these categories is the range of $MTTF_d$ values. Table 12 shows calculated and reference values. They are graphically displayed in figure 26 as well, reproduced at the end of this appendix for convenience.

Table 12 – Comparison between PFH values for category B and 1

	Category B			Category 1		
$MTTF_d$	ISO 13849	Calculated	Error	ISO 13849	Calculated	Error
3	3.80E-05	3.81E-05	0.2%	-	-	-
3.3	3.46E-05	3.46E-05	0.0%	-	-	-
3.6	3.17E-05	3.16E-05	-0.2%	-	-	-
3.9	2.93E-05	2.93E-05	0.0%	-	-	-
4.3	2.65E-05	2.66E-05	0.4%	-	-	-
4.7	2.43E-05	2.43E-05	0.0%	-	-	-
5.1	2.24E-05	2.24E-05	-0.1%	-	-	-
5.6	2.04E-05	2.04E-05	0.1%	-	-	-
6.2	1.84E-05	1.84E-05	-0.1%	-	-	-
6.8	1.68E-05	1.67E-05	-0.4%	-	-	-
7.5	1.52E-05	1.52E-05	-0.2%	-	-	-
8.2	1.39E-05	1.39E-05	0.0%	-	-	-
9.1	1.25E-05	1.25E-05	0.3%	-	-	-
10	1.14E-05	1.14E-05	0.2%	-	-	-
11	1.04E-05	1.04E-05	-0.3%	-	-	-
12	9.51E-06	9.50E-06	-0.1%	-	-	-
13	8.78E-06	8.76E-06	-0.2%	-	-	-
15	7.61E-06	7.60E-06	-0.1%	-	-	-
16	7.13E-06	7.11E-06	-0.3%	-	-	-
18	6.34E-06	6.33E-06	-0.1%	-	-	-
20	5.71E-06	5.71E-06	0.1%	-	-	-
22	5.19E-06	5.19E-06	-0.1%	-	-	-
24	4.76E-06	4.76E-06	0.0%	-	-	-
27	4.23E-06	4.24E-06	0.1%	-	-	-
30	-	-	-	3.80E-06	3.83E-06	0.7%
33	-	-	-	3.46E-06	3.47E-06	0.4%
36	-	-	-	3.17E-06	3.18E-06	0.4%
39	-	-	-	2.93E-06	2.94E-06	0.3%
43	-	-	-	2.65E-06	2.66E-06	0.5%
47	-	-	-	2.43E-06	2.44E-06	0.5%
51	-	-	-	2.24E-06	2.25E-06	0.5%
56	-	-	-	2.04E-06	2.05E-06	0.6%

Continued on next page

Table 12 – continued from previous page

$MTTF_d$	ISO 13849	Calculated	Error	ISO 13849	Calculated	Error
62	-	-	-	1.84E-06	1.86E-06	1.1%
68	-	-	-	1.68E-06	1.69E-06	0.5%
75	-	-	-	1.52E-06	1.53E-06	0.9%
82	-	-	-	1.39E-06	1.40E-06	0.8%
91	-	-	-	1.25E-06	1.26E-06	1.0%
100	-	-	-	1.14E-06	1.15E-06	0.8%

E.2.2 Category 3

Table 13 shows calculated and reference values.

Table 13 – Comparison between PFH values for category 3

	Category 3 with DC_{avg} of 60%			Category 3 with DC_{avg} of 90%		
$MTTF_d$	ISO 13849	Calculated	Error	ISO 13849	Calculated	Error
3	1.26E-05	1.58E-05	25.3%	6.09E-06	6.11E-06	0.4%
3.3	1.13E-05	1.42E-05	25.9%	5.41E-06	5.49E-06	1.5%
3.6	1.03E-05	1.29E-05	25.5%	4.86E-06	5.01E-06	3.0%
3.9	9.37E-06	1.19E-05	26.6%	4.40E-06	4.54E-06	3.1%
4.3	8.39E-06	1.06E-05	26.6%	3.89E-06	4.03E-06	3.5%
4.7	7.58E-06	9.55E-06	25.9%	3.48E-06	3.63E-06	4.2%
5.1	6.91E-06	8.76E-06	26.8%	3.15E-06	3.29E-06	4.3%
5.6	6.21E-06	7.80E-06	25.6%	2.80E-06	2.97E-06	6.1%
6.2	5.53E-06	6.91E-06	25.0%	2.47E-06	2.59E-06	4.9%
6.8	4.98E-06	6.22E-06	24.8%	2.20E-06	2.30E-06	4.3%
7.5	4.45E-06	5.50E-06	23.6%	1.95E-06	2.04E-06	4.6%
8.2	4.02E-06	4.91E-06	22.2%	1.74E-06	1.80E-06	3.2%
9.1	3.57E-06	4.29E-06	20.2%	1.53E-06	1.59E-06	1.7%
10	3.21E-06	3.84E-06	19.7%	1.36E-06	1.37E-06	0.5%
11	2.81E-06	3.34E-06	19.0%	1.18E-06	1.20E-06	1.6%
12	2.49E-06	2.99E-06	20.1%	1.04E-06	1.06E-06	1.6%
13	2.23E-06	2.66E-06	19.%	9.21E-07	9.35E-07	1.5%
15	1.82E-06	2.18E-06	19.7%	7.44E-07	7.45E-07	0.2%
16	1.67E-06	1.96E-06	17.5%	6.76E-07	6.99E-07	3.3%
18	1.41E-06	1.66E-06	18.0%	5.76E-07	5.85E-07	1.6%
20	1.22E-06	1.41E-06	15.5%	4.85E-07	5.02E-07	3.6%
22	1.07E-06	1.26E-06	17.4%	4.21E-07	4.29E-07	2.0%
24	9.47E-07	1.10E-06	15.9%	3.70E-07	3.74-07	1.0%
27	8.04E-07	9.06E-07	12.7%	3.10E-07	3.15E-07	1.6%
30	6.94E-07	7.75E-07	11.6%	2.65E-07	2.72E-07	2.7%
33	5.94E-07	6.45E-07	8.6%	2.30E-07	2.31E-07	0.3%
36	5.16E-07	5.54E-07	7.4%	2.01E-07	2.05E-07	1.9%

Continued on next page

Table 13 – continued from previous page

$MTTF_d$	ISO 13849	Calculated	Error	ISO 13849	Calculated	Error
39	4.53E-07	4.74E-07	4.6%	1.78E-07	1.79E-07	0.7%
43	3.87E-07	4.12E-07	6.6%	1.54E-07	1.49E-07	-3.3%
47	3.35E-07	3.62E-07	8.2%	1.34E-07	1.15E-07	1.0%
51	2.93E-07	3.10E-07	5.9%	1.19E-07	1.15E-07	-3.1%
56	2.52E-07	2.61E-07	3.6%	1.03E-07	1.03E-07	0.3%
62	2.13E-07	2.22E-07	4.3%	8.84E-08	8.62E-08	-2.5%
68	1.84E-07	1.92E-07	4.6%	7.68E-08	7.93E-08	3.3%
75	1.57E-07	1.61E-07	3.2%	6.62E-08	6.91E-08	4.3%
82	1.35E-07	1.37E-07	1.2%	5.79E-08	5.59E-08	-3.4%
91	1.14E-07	1.12E-07	-1.4%	4.94E-08	4.79E-08	-2.9%
100	1.01E-07	1.00E-07	-0.9%	4.29E-08	4.22E-08	-1.5%

E.2.3 Category 4

Table 14 shows calculated and reference values.

Table 14 – Comparison between PFH values for category 4

	Category 4		
$MTTF_d$	ISO 13849	Calculated	Error
30	9.54E-08	9.65E-08	1.1%
33	8.57E-08	8.90E-08	3.9%
36	7.77E-08	7.76E-08	-0.1%
39	7.11E-08	7.08E-08	-0.5%
43	6.37E-08	6.34E-08	-0.5%
47	5.76E-08	5.54E-08	-3.9%
51	5.26E-08	5.25E-08	-0.2%
56	4.73E-08	4.79E-08	1.4%
62	4.22E-08	4.22E-08	0.1%
68	3.80E-08	3.60E-08	-5.4%
75	3.41E-08	3.42E-08	0.4%
82	3.08E-08	3.42E-08	11.2%
91	2.74E-08	2.88E-08	5.0%
100	2.47E-08	2.45E-08	-0.6%

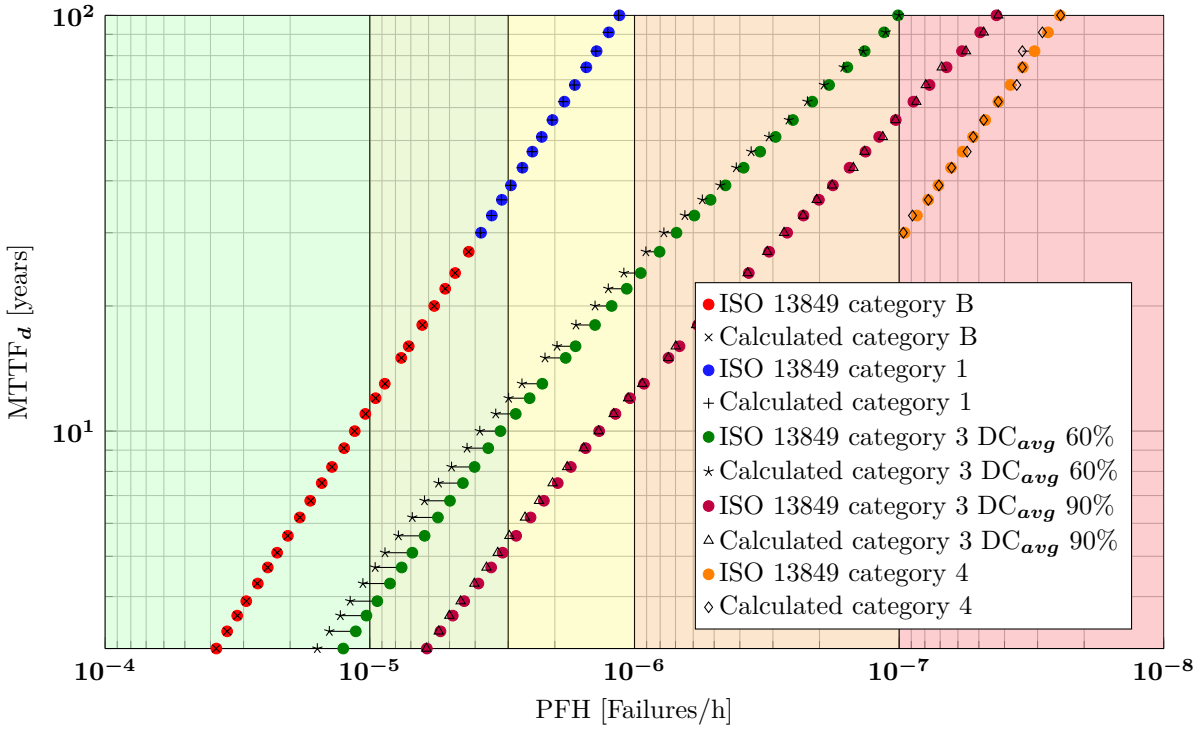

Figure 50 – Reproduction of figure 26. Comparison of PFH values of ISO 13849 and calculated through BlockSim for all calculated categories. Intervals that represent different Performance Levels are shaded in different colors.

REFERENCES

BILLINTON, R.; ALLAN, R. N. *Reliability Evaluation of Engineering Systems - Concepts and Techniques*. [S.l.]: Springer, 1992. ISBN 978-0306440632.

BOSCH REXROTH AG. *Reliability characteristics MTTFd for functional safety according to EN ISO 13849*. [S.l.], 3 2012.

BUJA, G.; MENIS, R. Dependability and functional safety. *IEEE Industrial Electronics Magazine*, p. 4–12, 2012.

DIAS, A. et al. *Metodologia para análise de risco : mitigação de perda de SF_6 em disjuntores*. [S.l.]: Eletrosul, 2013. ISBN 978-85-98128-42-9.

DORRA, M.; REINERT, D. *Annex 6: Quantitative Analysis of Complex Electronic Systems using Fault Tree Analysis and Markov Modelling*. [S.l.], February 2000.

EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION. *Directive 2006/42/EC of the European Parliament and of the Council of 17 May 2006 on machinery, and amending Directive 95/16/EC*. 2006.

GOBLE, W. M. *Control Systems Safety and Reliability*. Third edition. [S.l.]: ISA, 2010.

GONZALEZ, F. E. *Estudo das forças atuantes em mecanismos de regulação de ângulo de passo e desenvolvimento de um sistema emulador de cargas*. mathesis — Universidade Federal de Santa Catarina, 2012.

GUIDE to application of the Machinery Directive 2006/42/EC. [S.l.], June 2010.

HAUKE, M. et al. *Functional machine of machine controls - Application of EN ISO 13849* -. [S.l.], June 2009. Disponível em: <http://www.dguv.de/ifa/Publikationen/Reports-Download/BGIA-Reports-2007-bis-2008/BGIA-Report-2-2008/index-2.jsp>.

IAEA. *Accidental overexposure of radiotherapy patients in San Jose, Costa Rica*. Vienna, June 1998.

INNAL, F. et al. New insight into the average probability of failure on demand and the probability of dangerous failure per hour of safety instrumented systems. *Proceedings of the Institution of Mechanical Engineers, Part O: Journal of Risk and Reliability*, v. 224, p. 75–86, 2010.

International Electrotechnical Comission. *IEC 61508-4 ed2.0 - Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 4: Definitions and abbreviations*. 2010.

International Electrotechnical Comission. *IEC 61508-6 ed2.0 - Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 6: Guidelines on the application of IEC 61508-2 and IEC 61508-3*. 2010.

International Organisation for Standardization. *ISO 13849-1:2006 - Safety of machinery - Safety-related parts of control systems - Part 1: General principles for design*. 2006.

International Organisation for Standardization. *ISO 12100:2010 - Safety of machinery - General principles for design - Risk assessment and risk reduction*. 2010.

International Organisation for Standardization. *ISO/TR 22100-2:2013 - Safety of machinery - Relationship with ISO 12100 - Part 2: How ISO 12100 relates to ISO 13849-1*. 2013.

JIN, H. *A contribution to reliability assessment of safety-instrumented systems*. Tese (Doutorado) — Norwegian University of Science and Technology, 2013.

JOCELYN, S. et al. Feasibility study and uncertainties in the validation of an existing safety-related control circuit with the iso 13849-1:2006 design standard. *Reliability Engineering and System Safety*, v. 121, p. 104–112, 2014.

KUHLHOFF, I. R.; MORENO, U. F.; ORTH, A. Aplicação da norma iso 13849 de segurança funcional de uma bancada de testes hidráulica. In: *Anais do congresso Brazil Automation 2014*. [S.l.: s.n.], 2014.

KUMAMOTO, H.; HENLEY, E. J. *Probabilistic Risk Assessment and Management for Engineers and Scientists*. [S.l.]: Wiley-IEEE Press, 2000. 620 p. ISBN 0780360176.

LERéVéREND, P. Inside the standardization jungle: Iec 62061 and iso 13849-1, complementary or competing? In: . [S.l.: s.n.], 2008. p. 1–5.

LEVESON, N. Medical devices: The therac-25. In: *Safeware: System Safet and Computers*. Addison-Wesley, 1995. ISBN 0-201-11972-2. Disponível em: <http://sunnyday.mit.edu/>.

MIKELSONS, L.; SU, Z. Simulation for verification and validation of functional safety. In: *Proceedings of the 10th International Modelica Conference*. [S.l.: s.n.], 2014.

MINISTéRIO DA PREVIDêNCIA SOCIAL. *Anuário Estatístico da Previdência Social 2013*. [S.l.], 2014.

MINISTERIO DO TRABALHO E EMPREGO. *Portaria n 1.893 de 9 de dezembro de 2013 - NR 12. Altera a Norma Regulamentadora NR12 - Seguranca no trabalho em maquinas e equipamentos.* 2013.

NEGRI, V. J. de. *Introdução aos Sistemas para Automação e Controle Indutrial*. 2005.

NTSB. *AIRCRAFT ACCIDENT REPORT UNITED AIRLINES FLIGHT 232 MCDONNELL DOUGLAS DC-1010 SIOUX GATEWAY AIRPORT SIOUX CITY, IOWA JULY 19, 1989*. [S.l.], November 1990. Disponível em: <http://www.airdisaster.com/reports/ntsb/AAR90-06.pdf>.

ORTH, A.; BARG, J. Reliability is required: new safety standards for machine control systems. *Control Engineering*, p. M3–M5, 2010.

ORTH, A. et al. *10 steps to performance level. Handbook for the implementation of functional safety according to ISO 13849*. [S.l.]: Bosch Rexroth AG, 2012. ISBN 978-3-9814879-2-3.

ORTH, A.; RAKSCH, C. Determination of reliability parameters of hydraulic components for safety applications in industrial and mobile machines. In: *Proceedings of the 9th International Fluid Power Conference (IFK)*. Aachen, Germany: [s.n.], 2014. v. 2, p. 144–153.

ORTH, A.; SWAGTEN, G.; SILVA, R. O. Contributions of functional safety in the design of safe and reliable marine and offshore system. In: BIOCOMBUSTÍVEIS, I. B. de Petróleo Gás e (Ed.). *Proceedings of RIO OIL & GAS 2014 Expo and Conference*. [S.l.: s.n.], 2014.

RAUSAND, M. *Reliability of Safety-Critical Systems*. [S.l.]: Wiley, 2014. ISBN 978-1-118-55337-4.

RIGDON, S. E.; BASU, A. P. *Statistical Methods for the Reliability of Repairable Systems*. [S.l.]: Wiley-Interscience, 2000. 224 p. ISBN 978-0-471-34941-9.

ROUVROYE, J.; BLIECK, E. Comparing safety analysis techniques. *Reliability Engineering and System Safety*, v. 75, p. 289–294, 2002.

SCHAERFER, M.; BORK, T. Tangible and transparent use of reliability data for functional safety, "the sense and nonsense of quantification". In: *SIAS2007*. [S.l.: s.n.], 2007.

SCHUMACHER, J.; RüCKWART, W. Will it work? fluid power and functional safety. In: *Proceedings of the International fluid power conference*. Aachen: [s.n.], 2014. p. 488–494.

SKLET, S. Safety barriers: Definition, classification, and performance. *Journal of Loss Prevention in the Process Industries*, v. 19, p. 494–506, 2006.

TRAUFETTER, G. *San Francisco: Crash 'Was Only a Matter of Time'*. July 2013. Disponível em: <http://www.spiegel.de/international/world/pilots-missing-control-systems-led-to-san-francisco-crash-a-909956.html>.